**Information Technology Considerations**

**Levels of System Access and Potential Risks**

|  |  |  |
| --- | --- | --- |
| **System Access** | **Action Allowed** | **Potential Risk** |
| Create transactions | The user records data and documents the transaction. | The data created is:  Misleading  Fraudulent  Used for unintended purposes |
| Data inquiry | The user is given access to “view” data only. | The data is disclosed to unauthorized individuals. |
| Modify transactions | The user changes existing data. | The integrity of the data is compromised, thereby affecting the reliability of the data for its intended purpose.  The data was changed to conceal a fraudulent transaction. |
| Delete transactions | The user temporarily or permanently destroys data. | The data is not available to the system owner and other authorized users.  The data was destroyed to conceal a fraudulent transaction. |

**IT General Control Objectives for Financial Reporting**

|  |
| --- |
| **Financial Systems Are Aligned With IT And Business Strategies** |
| **Alignment of Financial Systems with IT Strategy and Initiatives**  What is the agency’s IT and information systems strategy with respect to financial systems? Does this strategy align with statewide strategies and directives?  What specific IT policies exist, both at the agency level and statewide? What specific federal and state laws, regulations or other pronouncements may apply? Who is responsible for compliance? |
| **Organization of the Agency IT Function**  How is the agency IT function organized?  Is the IT function centralized or decentralized? Who is responsible for financial systems?  Who is head of the IT organization and to whom does he/she report?  Have there been any significant personnel changes during the year that might affect the amount or quality of support for financial systems?  Does the support of financial systems involve external parties, such as outsourcing, vendors or consultants?  **Project Management**  Does the IT function have a uniform project management model that is followed for all projects, including acquisition of financial system applications?  Do significant projects require a business benefit assessment?  Are clear deliverables defined in the project?  Are the projects formally controlled against both budgets and quality?  What measures for quality exist?  Are there significant financial systems activities outside the IT function? |
| **Staffing Levels**  Is the number of IT staff and their skill level in line with the agency’s financial systems requirements?  How much of the financial systems are owned and maintained by the users? Do they have the appropriate knowledge to exercise their ownership?  How great is the reliance on key IT staff members or key users? |
| **Alignment of Financial Systems to Business Strategies and Objectives**  Does the financial system meet the needs of agency management? How accurate and useful is the financial systems information for the agency?  How old are the financial systems? Will they need upgrades or replacements in the near future? How much does it cost for maintenance, staff, and support to keep the financial applications going on a day-to-day basis?  How much does the agency rely on suppliers to perform maintenance?  Who is responsible for financial applications? Do these people have sufficient knowledge?  How is the financial information stored and retrieved? Does the financial system provide for a proper audit trail?  What financial business information demands are not covered by the existing system? What is being done to meet the unfulfilled demands?  Are there back up/recovery procedures and contingency plans to ensure that critical financial processing is maintained and that financial data is safeguarded in times of disaster or emergencies? |
| **Significant Changes/Known Problems With Financial Systems Are Documented** |
| **Financial Systems Changes**  What new financial systems have been implemented? How significant are the new systems to the agency’s business? (For example, are key business processes to be performed electronically over the internet?) Is maintenance to be performed internally or by suppliers?  How well did the implementation go? Is there documentation of the testing, problems identified and how they were resolved? Were there any problems with data conversion?  Have there been changes to existing financial systems? Are they significant? Have there been any significant upgrades to the system software? Have there been significant changes to the network? Were any problems encountered? Is there documentation of how the problems were handled?  Have there been changes to the automated controls within the financial system?  Has there been a migration to a new environment? Web-based, for example?  Was the internal audit function involved in the changes? Were any pre- or post-implementation reviews performed? |
| **Known Problems in Financial Systems**  Have significant problems of deficiencies affecting the functionality of financial systems been identified? If so, are work-around procedures in place and have they been documented?  Have there been significant operational failures, security incidents or data corruption? How were these situations handled? Have reports been issued by internal audit or other IT personnel? |
| **Development/Implementation Controls Are Clearly Defined And Documented** |
| **Overall Control Activities**  Does the agency have a formal system development life cycle (SDLC) methodology that must be followed?  Has a detailed project plan been developed which has?  Clearly defined goals and tasks  Timelines and milestones  Sponsor approval for each milestones  Projected roles, responsibilities and resources?  Are project status reports to management required on an ongoing basis that include:  Assessments of quality assurance review  Actual completion of tasks against plan  Actual delivery dates against milestones and deadlines  Actual project costs against budgets? |
| **Only Appropriate Financial Systems Projects are Undertaken**  Does the financial systems project have a clear business objective with well-defined scope and boundaries?  Has a cost-benefit analysis been done? Are the benefits specific and quantifiable or are they vague?  Does the project have a clear sponsor/owner from senior management?  Does the project team have sufficient relevant business and technical expertise to complete the project? |
| **Analysis and Design Control Activities**  Are the business specifications clearly defined in sufficient detail? Does the project team understand them?  Are technical specifications clearly defined? Do they include requirements for system functionality, capacity and performance, security design and processing controls?  Do technical specifications include requirements associated with interfaces to statewide financial systems?  Have appropriate application controls such as robust edits and validations, exception reporting and control totals been included in the design?  Is process and data modeling performed?  Is data conversion necessary?  How are changes to the original design approved and controlled? |
| **Control Activities Over Internal Development and Package Selection for New Applications**  Does internal development or the package selected for new financial applications employ standard coding methodologies?  What controls or tools are utilized to ensure that all dependencies between integrated applications are identified and considered?  For purchased financial systems software packages, is the package selected widely used and does the vendor have a reputation for providing robust support services?  For purchased financial systems software packages is customization required? How is this controlled? |
| **Testing and Quality Assurance Control Activities**  To what extent are separate environments maintained for development, testing and production?  Are users involved in the testing? Is user management required to authorize acceptance of the system?  What controls are in place to prevent or detect unauthorized changes to code after testing is complete but before going live? What ensures that configuration options and parameters set meet the business objectives and control requirements? |

|  |
| --- |
| **Data Conversion Control Activities**  What procedures ensure that the mapping of data fields from the legacy system to the target system is correct?  What ensures the quality of the converted data in terms of:  Accuracy  Integrity  Consistency  Completeness  Accessibility  Existence  What ensures that critical system interfaces are modified to accept the new data model? |
| **Control Activities Over Going Live**  Is approval from the project sponsor/owner and IT management required for authorizing the go-live decision? Is this authorization formal?  Are quality assurance reviews required as part of the go-live decision making process?  Does the agency have a go-live checklist?  How does the agency ensure that only the properly tested, reviewed and approved version of the system is transferred to the live environment?  Does the agency have a process to communicate the specifics of the go-live process?  Have individuals from both the financial organization and IT been designated to support the new system during the go-live period.  Is a post-implementation review planned? |
| **Documentation and Training Control Activities**  Are there policies to ensure that both user and technical documentation is developed for all new financial systems and is this documentation available at time of implementation?  To what extent have users and computer operators received adequate training on the new financial system? Is there a formal training program to facilitate training? |

|  |
| --- |
| **Change Management Controls Are Clearly Defined and Documented** |
| **Management of Change Activities**  Has management established a process with documented policies and procedures for managing changes to financial systems?  How does management monitor progress and ensure that approved changes are implemented on a timely basis?  Does IT management use reports/statistics to review the operational quality of the financial systems?  How does IT accomplish the installation of infrastructure-related patches for hardware and software? Are subcontractors utilized? |
| **Control Activities Over Approval and Tracking of Change Requests**  Are all requests for changes to existing financial systems captured and managed centrally? Are there controls in place to log all requests and track them?  Who approves and prioritizes the change requests? How is approval and prioritization recorded?  Does the order in which changes are implemented reflect the priorities assigned to them?  Are developers in close contact with users? To what extent are there adequate procedures in place to ensure that developers understand the users’ requirements before making program changes to financial applications? |
| **Control Activities Over Construction of System Changes**  Are programmers following standard coding methodologies?  What controls are in place to ensure the source code used is the most recent version and modifications by more than one programmer are coordinated?  What controls or tools are utilized to ensure that all dependencies between integrated applications are identified and considered?  How do programmers ensure that a standard configuration is used across all maintenance efforts? |
| **Testing and Quality Assurance Control Activities Related to System Changes**  To what extent are separate environments maintained for development, testing and production?  Are users involved in the testing? Is user management required to authorize acceptance of the system?  What controls are in place to prevent or detect unauthorized changes to code after testing is complete but before going live? What ensures that configuration options and parameters set meet the business objectives and control requirements? |
| **Control Activities Over Going Live with System Changes**  How are scheduled and non-emergency changes migrated into the production environment?  How are emergency changes migrated into the production environment? What is the process by which users authorize the emergency changes?  To what extent do developers have “write” access to the production environment and is this access logged?  What processes and controls ensure that current production libraries/directories are updated with the correct version of the program?  What processes and controls ensure that changes do not compromise security controls (e.g., checking software to ensure it does not contain malicious code, such as a “Trojan Horse” or a virus)?  What procedures exist to ensure that all changes have adequate back-out procedures defined with management approved escalation steps? |
| **Documentation and Training Control Activities Related to System Changes**  Are there procedures to update user documentation/procedures for changes to financial systems?  Are there procedures to update technical documentation/procedures for changes to financial systems?  To what extent have the users and computer operators received adequate training concerning the newly implemented changes? |
| **Security Control Activities Are Clearly Defined and Communicated** |
| **Security Organization and Management**  Has management considered the appropriate segregation of duties among personnel involved in the IT security function? Have roles and responsibilities been clearly defined and communicated?  Is the financial system’s business owner management appropriately included in the design of the IT security function from a data ownership perspective? |
| **Security Policies and Procedures**  Has management published a complete set of policies and procedures that support the information integrity objectives of the agency?  Does management have a controlled process in place to update the security policy and procedure documentation on a periodic basis?  Has management established a process to ensure that IT and business users receive adequate, appropriate, education and training regarding security policies and procedures, as well as their specific security responsibilities, on a periodic basis? |
| **Security Over Financial Applications**  Is a formal documented security administration process in place to ensure that all application access, including access to financial applications, is approved?  Does the security administration process require business unit management approval of all access to financial applications and financial data “owned” by that business unit?  Does the centralized security administration function facilitate periodic reviews of user access by business unit management to ensure that access remains commensurate with job responsibilities over time? |
| **Security over Financial Data**  Has management implemented a formal process for changing financial data access settings (i.e., data file permissions) in a controlled manner?  Has management implemented a formal security administration process for granting, changing and removing direct access to financial data in a controlled manner?  Does management periodically review direct financial data access (i.e., Database Administrator access) to ensure that the access remains commensurate with job responsibilities?  If direct financial data access is controlled using special system utilities, is the use of such utilities documented, logged and reviewed on a regular basis?  Are appropriate monitoring and audit trail controls designed to allow management to monitor the data environment for potential unauthorized activity?  Does management periodically review monitoring reports to identify potential unauthorized activity? What actions are taken when potential unauthorized activity is identified?  Has management complied with federal and state laws, regulations and rules regarding the privacy and confidentiality of financial data collected from customers, vendors, employees?  Does each system produce a report showing all authorized users and their associated roles/permissions?  Has the responsibility for transactional records retention been assigned to the application owners? |
| **Physical Security Over Financial Systems**  How is physical access to agency buildings/sites restricted (consider any location where computer facilities are located; also any locations connected to those facilities via the agency’s internal networks)?  How is physical access to data centers restricted?  How is physical access to remote data centers/server rooms restricted?  How is physical access to wiring closets and other sensitive physical network locations/components restricted?  How is physical access to removable storage media (e.g., tapes, optical discs, etc.) restricted?  How well secured is sensitive financial system documentation? |

**IT application control objectives for financial reporting**

|  |
| --- |
| **Data Processed Are Properly Authorized** |
| **All Financial Application Users are Appropriately Identified and Authenticated**  Are passwords and personal user IDs required? Are passwords required to be changed at regular intervals? Are users notified that passwords will expire soon?  Do sign-on mechanisms limit the number of unsuccessful sign-on attempts?  Do sign-on mechanisms advise users of the date/time of their last successful sign-on?  Do sign-on mechanisms display and validate sign-on information only after it has all been entered?  Are “nonrepudiation” controls in place that prevent senders and receivers of information from denying that they sent or received the information?  Is the agency exploring emerging technologies such as digital certificates or smart cards? |
| **Access to Financial Application and Related Data Files is Restricted**  Is a logical access control system in place that restricts access to the application and data to authorized users based on the users’ individual roles?  Are system administrators subject to strong authentication controls?  Are access rights authorized by the application “owner”?  Are access rights revoked promptly when the user in no longer entitled to them?  Have firewalls been established to protect the application and data from unauthorized use?  Do terminals automatically disconnect from the system when not used after a specified period of time?  Is the computer equipment located in physically secure locations?  Is manual intervention minimized by designing automated processes?  Is information about the internal workings of the financial application (e.g., application responses or error messages) prevented from being disclosed?  Do access logs include sufficient information to provide a satisfactory audit trail (including users’ identities and locations, dates/times of access, and particular files or system utilities accessed) which is reviewed periodically to identify dubious activity and determine responsibility for particular events?  Are access logs retained for the specified period needed to comply with legal and regulatory requirements? |
| **All Data Are Authorized Before Entering the Financial Application**  Is critical input information tested against predefined criteria? Are exceptions reviewed by an individual with proper authority to approve them?  Is paper-based information reviewed and approved prior to input? |
| **Data Processed Are Complete** |
| **All Authorized Data is Entered and Processed by the Application.**  Are transactions numbered prior to entry? Is the sequence checked periodically?  Are control totals, hash totals, and record counts used to ensure that all data are processed?  Is transaction data matched with the data in a master or suspense file? Are unmatched items from both the transaction data and master or suspense file reported for investigation?  Is the completeness (and accuracy and validity) of processed information confirmed by an independent means, such as comparing to bank statements, customer/supplier records, or physical stock? |
| **Data Processed Are Accurate** |
| **Data Entry Design Features**  Are data entry screens preformatted?  Is the data input process menu-driven?  Is information input electronically? |
| **Data Validation and Editing**  Are automated validation and edit checks (such as check digits, limit tests, reasonableness checks) included in the application design? |
| **Erroneous Data**  Are suspense files used to capture and control errors?  Are the suspense files reviewed regularly and errors appropriately resolved?  Are error and exception reports built into the application?  Are key fields or files write-protected, so that information cannot be accidentally overwritten?  Are plausibility checks performed to ensure output is reasonable? |
| **Confidential Information Is Protected** |
| **Access to Financial Application Output is Restricted**  Is access to confidential information limited to authorized individuals consistent with the entity’s confidentiality policies?  Are data encryption technologies used to protect the transmission of user authentication, verification, and confidential information? |
| **Change Management Controls Are in Place** |
| **Change Management Process**  Is there a change management process in place that is documented?  Are change requests documented? Are possible impacts evaluated in terms of risk? Are changes approved by the application “owner”?  Prior to going live are changes tested and reviewed to ensure they do not contain malicious code or a virus that would compromise security controls?  Are back-out positions established so that changes can be backed out if they fail?  Once changes have been made, are there arrangements to ensure that version control is maintained, a record is maintained showing what was changed, when and by whom, and the details of the changes are communicated to relevant individuals?  Are checks performed on a regular basis to confirm that only approved changes have been made (by using code comparison programs or checking “before and after” contents of key records, such as customer master files)? |
| **Incident Management Controls Are In Place** |
| **Incident Management Process**  Does an incident management process exist that is documented and covers reporting, investigating  and resolving incidents (including malicious attacks, abuse/misuse of financial systems by staff, loss of power/communications services and errors by users or computer staff)?  Are incidents reported to a single point of contact, such as a help desk, documented and prioritized?  Does the resolution of incidents include investigating root causes, planning corrective actions, and performing a review to ensure that the security of the financial application has not been affected?  Are patterns of incidents reviewed to identify potential security breaches and to minimize the chances of disrupting other applications? |
| **Business Continuity Plan Is Documented And Tested** |
| **Business Continuity Planning**  Is the financial application supported by a documented business continuity plan?  Does the business continuity plan specify recovery tasks to be carried out, responsibilities of specified individuals, and arrangements for safe storage of plans and their retrieval in emergencies?  Does the business continuity plan address the prolonged unavailability of key business information and backup files; computer or network equipment; key personnel; power, communications and other vital services; access to buildings and facilities?  **Business Continuity Testing**  Have steps been taken to ensure business continuity arrangements will work within critical timeframes by testing alternative processing arrangements and carrying out realistic simulations? |
| **Essential Information/Software Used By Financial Applications Are Backed Up** |
| **Backup Procedures**  Are backups performed on a regular basis according to a defined cycle?  Are backups performed using a back-up management package?  Are backups verified to ensure that back-up versions can be restored successfully?  Are backups protected from loss, damage and unauthorized access?  Are backups maintained at an off-site location for disaster recovery? |
| **Business Requirements for Service Providers are Defined** |
| **Service Agreements**  Are documented service agreements used to define the computer and network services required to support the financial application?  Does the service agreement specify the roles and responsibilities of the service provider and the financial application “owner”?  Does the service agreement specify capacity requirements, such as normal and peak loads, response times, and maximum permissible down-time?  Does the service agreement specify security controls, including:  Access restrictions  Authentication methods  A change management process  An incident management process  Continuity of services arrangements  Segregation of duties?  Is independent confirmation of the operation of the service provider’s security controls obtained?  Is the achievement of service targets periodically reviewed? |
| **Financial Applications Are Subject to Security Audits** |
| **Independent and Regular Security Audits**  Is the financial application subject to **independent** and regular security audits/reviews that assess the status of information security in all key areas, including application management, the user environment, system management and special areas (e.g., third party access, cryptographic key management)?  Is security audit activity controlled by restricting, monitoring and logging the activities of the audit team?  Are the recommendations resulting from security audits reviewed with the financial application owner and reported to top management? |
| **Third Party Connections Are Subject to Additional Controls** |
| **Third Party Access Arrangements**  Are third party access arrangements subject to risk assessment, approved by the financial application “owner,” and agreed by both parties in a documented agreement?  Do risk assessments of third party access arrangements take the following conditions into account?  Criticality and sensitivity of information and systems to be accessed  Status of the third party (well established versus new, relatively unknown)  Type of business process to be performed by third parties (e.g., information retrieval, order submission, funds transfer or remote maintenance)  Technical aspects of connection  Vulnerabilities in third party networks, applications or operating systems  Restrictions imposed by legal or regulatory requirements  Lack of control over the staff and system components employed by third parties  Obligations to third parties to provide reliable service and timely, accurate information  Do third party agreements include the following?  Timeframes for completion of transactions and arrangements for ensuring that transactions cannot be repudiated (e.g., by using “digital signatures”)  Agreed security controls (e.g., access mechanisms, virus protection and back-up)  Arrangements for managing changes and incidents  The right to audit security arrangements within the third party  Non-disclosure of information  A requirement to return or destroy information or software at an agreed point  The respective liabilities of the parties to the agreement  Protection of intellectual property rights  The right to monitor and revoke user activity |
| **Cryptographic Keys Are Tightly Managed** |
| **Standards, Procedures and Responsibilities**  Are cryptographic keys managed in accordance with documented standards and procedures?  Do the standards and procedures cover:  Selection of sufficient lengths of cryptographic keys  Secure distribution, storage and periodic updating  Revocation of cryptographic keys when a recipient changes job  Recovery of cryptographic keys that are lost, corrupted or expired  Management of cryptographic keys that have been compromised  Archival of cryptographic keys and maintenance of cryptographic key history  Defined activation/de-activation dates?  Have responsibilities for protecting cryptographic keys against unauthorized access or destruction been clearly assigned? |
| **Public Key Infrastructure (PKI) Used by the Financial Application is Protected** |
| **Standards, Procedures and Responsibilities**  Are documented standards/procedures established, which define  The process required to manage cryptographic keys/digital certificates within the PKI  Methods required to operate the PKI  Actions to be taken in the event of a compromise?  Are PKI users fully aware of the purpose and function of PKI, their responsibility to protect private keys, and how to use the “digital signatures”?  **Certification Authority**  Has an internal Certification Authority (people, processes and tools) been established to create issue and manage the public key certificates that are used within a PKI?  Is the Certification Authority protected by strong access control mechanisms and strong authentication?  Has the Certification Authority been protected by “hardening” underlying operating systems?  **Disaster Recovery**  Has a contingency plan been developed for the financial application supported by the PKI that includes methods of recovering the PKI in the event of a disaster? |
| **Web-Enabled Applications Are Supported by Specialized Technical Controls** |
| **Accreditation**  Have business practices and privacy policies applicable to the web sites associated with the financial application been independently accredited (for example, by Web Trust or TRUSTe)?  **Web Servers and Connections Between Web Servers and Back-Office Systems**  Are the web servers that support the financial application located in an area that is isolated from the Internet and internal networks by firewalls?  Run on one or more dedicated computers?  Run with “least privileges,” meaning that high-level privileges are excluded, such as “Administrator” for Windows NT systems or “Root” for UNIX systems?  Prevented from initiating network connection to the internet?  Configured so that scripts can only be run from specified locations?  Is the connection between web servers and back-office systems  Protected by firewalls?  Restricted to those services that are required by the application?  Restricted to code generated by web server applications, rather than by client applications?  Based on documented application programming interfaces (APIs)?  Supported by mutual authentication?  Are user accounts on back-office systems used by web servers to make connections run with “least privilege”?  Validation/Encryption of Information and Transaction Processing  Is information used by the application protected against corruption or disclosure by performing input validation at the server, rather than just on the client application?  Encrypting sensitive data in transit (e.g., by using SSL or HTTPS)?  Are transaction processing monitors used to manage the execution, distribution and synchronization of transactions? |