CHAPTER 14

INFORMATION TECHNOLOGY CONTROLS

SCOPE

This chapter addresses requirements common to all financial accounting systems and is not limited to the statewide PeopleSoft financial accounting system, but also applies to subsystems used by the various agencies of the State of Indiana to process accounting information.

In the event these requirements are not met by the computer environment of the accounting system, compensating manual controls must be implemented.

Table of Contents

14.1 AUDITING STANDARDS

In accordance with Statements on Auditing Standards Number 122, issued by the American Institute of Certified Public Accountants (AICPA), the State Board of Accounts may review applicable computer systems that process accounting data. Consideration in the selection of the computer systems to be reviewed includes but is not limited to total dollars processed by the computer system, the complexity of the processing, the availability of alternate sources for audit information, and the criticality of non-financial information processed. The Information Technology Services (IT) controls reviewed will be based primarily on The Green Book from the Government Accountability Office (GAO), the Control Objectives for Information and Related Technologies (COBIT 5) from the Information Systems Audit and Control Association (ISACA), and the Global Technology Audit Guide (GTAG) 8: Auditing Application Controls from the Institute of Internal Auditors (IIA). Additional sources of information used in State Board of Accounts' IT reviews include but are not limited to publications of the AICPA and hardware and software vendors.

14.2 INTERNAL CONTROLS

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.

Segregation of duties is the concept of having different people do different tasks within the organization. It provides the foundation of good internal control by assuring that no one individual has the capability to perpetuate and conceal errors or irregularities in the normal course of their authorized duties. Segregation of duties is achieved within information technology systems by appropriate assignment of security profiles that define the data the users can access and the functions that they can perform. Access must be restricted to the minimum required for the user to perform their job function. Access rights must be periodically reviewed and approved by management.

14.3 DESIGN ACTIVITIES FOR THE INFORMATION SYSTEM (THE GREEN BOOK)

Principle 11 of the GAO's The Green Book states that management should design the entity's information system and related control activities to achieve objectives and respond to risks. The following attributes contribute to the design, implementation, and operating effectiveness of this principle: Design of the Entity's Information System, Design of Appropriate Types of Control Activities, Design of Information

Technology Infrastructure, Design of Security Management, and Design of Information Technology Acquisition, Development, and Maintenance. The Green Book reference number is in bold font.

14.3.1 Design of the Entity's Information System

11.02 *Management designs the entity's information system to respond to the entity's objectives and risks.*

11.03 *Management designs the entity's information system to obtain and process information to meet each operational process's information requirements and to respond to the entity's objectives and risks. An information system is the people, processes, data, and technology that management organizes to obtain, communicate, or dispose of information. An information system represents the life cycle of information used for the entity's operational processes that enables the entity to obtain, store, and process quality information. An information system includes both manual and technology-enabled information processes. Technology-enabled information processes are commonly referred to as information technology. As part of the control environment component, management defines responsibilities, assigns them to key roles, and delegates authority to achieve the entity's objectives. As part of the risk assessment component, management identifies the risks related to the entity and its objectives, including its service organizations; the entity's risk tolerance; and risk responses. Management designs control activities to fulfill defined responsibilities and address the identified risk responses for the entity's information system.*

11.04 *Management designs the entity's information system and the use of information technology by considering the defined information requirements for each of the entity's operational processes. Information technology enables information related to operational processes to become available to the entity on a timelier basis. Additionally, information technology may enhance internal control over security and confidentiality of information by appropriately restricting access. Although information technology implies specific types of control activities, information technology is not a "stand-alone" control consideration. It is an integral part of most control activities.*

11.05 *Management also evaluates information processing objectives to meet the defined information requirements. Information processing objectives may include the following:*

- *Completeness - Transactions that occur are recorded and not understated.*
- *Accuracy - Transactions are recorded at the correct amount in the right account (and on a timely basis) at each stage of processing.*
- *Validity - Recorded transactions represent economic events that actually occurred and were executed according to prescribed procedures.*

14.3.2 Design of Appropriate Types of Control Activities

11.06 *Management designs appropriate types of control activities in the entity's information system for coverage of information processing objectives for operational processes. For information systems, there are two main types of control activities: general and application control activities.*

11.07 *Information system general controls (at the entity-wide, system, and application levels) are the policies and procedures that apply to all or a large segment of an entity's information systems. General controls facilitate the proper operation of information systems by creating the environment for proper operation of application controls. General controls include security management, logical and physical access, configuration management, segregation of duties, and contingency planning.*

11.08 *Application controls, sometimes referred to as business process controls, are those controls that are incorporated directly into computer applications to achieve validity, completeness, accuracy, and confidentiality of transactions and data during application processing. Application controls include controls over input, processing, output, master file, interface, and data management system controls.*

14.3.3 Design of Information Technology Infrastructure

11.09 *Management designs control activities over the information technology infrastructure to support the completeness, accuracy, and validity of information processing by information technology. Information technology requires an infrastructure in which to operate, including communication networks for linking information technologies, computing resources for applications to operate, and electricity to power the information technology. An entity's information technology infrastructure can be complex. It may be shared by different units within the entity or outsourced either to service organizations or to location-independent technology services. Management evaluates the objectives of the entity and related risks in designing control activities for the information technology infrastructure.*

11.10 *Management continues to evaluate changes in the use of information technology and designs new control activities when these changes are incorporated into the entity's information technology infrastructure. Management also designs control activities needed to maintain the information technology infrastructure. Maintaining technology often includes backup and recovery procedures, as well as continuity of operations plans, depending on the risks and consequences of a full or partial power systems outage.*

14.3.4 Design of Security Management

11.11 *Management designs control activities for security management of the entity's information system for appropriate access by internal and external sources to protect the entity's information system. Objectives for security management include confidentiality, integrity, and availability. Confidentiality means that data, reports, and other outputs are safeguarded against unauthorized access. Integrity means that information is safeguarded against improper modification or destruction, which includes ensuring information's nonrepudiation and authenticity. Availability means that data, reports, and other relevant information are readily available to users when needed.*

11.12 *Security management includes the information processes and control activities related to access rights in an entity's information technology, including who has the ability to execute transactions. Security management includes access rights across various levels of data, operating system (system software), network, application, and physical layers. Management designs control activities over access to protect an entity from inappropriate access and unauthorized use of the system. These control activities support appropriate segregation of duties. By preventing unauthorized use of and changes to the system, data and program integrity are protected from malicious intent (e.g., someone breaking into the technology to commit fraud, vandalism, or terrorism) or error.*

11.13 *Management evaluates security threats to information technology, which can be from both internal and external sources. External threats are particularly important for entities that depend on telecommunications networks and the Internet. External threats have become prevalent in today's highly interconnected business environments, and continual effort is required to address these risks. Internal threats may come from former or disgruntled employees. They pose unique risks because they may be both motivated to work against the entity and better equipped to succeed in carrying out a malicious act as they have greater access to and knowledge of the entity's security management systems and processes.*

11.14 *Management designs control activities to limit user access to information technology through authorization control activities such as providing a unique user identification or token to authorized users. These control activities may restrict authorized users to the applications or functions commensurate with their assigned responsibilities, supporting an appropriate segregation of duties. Management designs other*

control activities to promptly update access rights when employees change job functions or leave the entity. Management also designs control activities for access rights when different information technology elements are connected to each other.

14.3.5 Design of IT Acquisition, Development, and Maintenance

11.15 *Management designs control activities over the acquisition, development, and maintenance of information technology. Management may use a systems development life cycle (SDLC) framework in designing control activities. An SDLC provides a structure for a new information technology design by outlining specific phases and documenting requirements, approvals, and checkpoints within control activities over the acquisition, development, and maintenance of technology. Through an SDLC, management designs control activities over changes to technology. This may involve requiring authorization of change requests; reviewing the changes, approvals, and testing results; and designing protocols to determine whether changes are made properly. Depending on the size and complexity of the entity, development of information technology and changes to the information technology may be included in one SDLC or two separate methodologies. Management evaluates the objectives and risks of the new technology in designing control activities over its SDLC.*

11.16 *Management may acquire information technology through packaged software from vendors. Management incorporates methodologies for the acquisition of vendor packages into its information technology development and designs control activities over their selection, ongoing development, and maintenance. Control activities for the development, maintenance, and change of application software prevent unauthorized programs or modifications to existing programs.*

11.17 *Another alternative is outsourcing the development of information technology to service organizations. As for an SDLC developed internally, management designs control activities to meet objectives and address related risks. Management also evaluates the unique risks that using a service organization presents for the completeness, accuracy, and validity of information submitted to and received from the service organization.*

14.4 ENTITY LEVEL CONTROLS (COBIT 5)

Entity-level controls are internal controls that help to ensure that management directives pertaining to the entire entity are carried out. They set the tone and culture of the governmental unit. Controls include, but are not limited to, the following:

- *Controls related to the overall control environment.*
- *Controls over management override.*
- *The governmental entity's risk assessment process.*
- *Centralized processing and controls, including shared service environments.*
- *Controls to monitor results of operations.*
- *Controls to monitor other controls, including activities of the internal audit function, the audit committee and self-assessment programs.*
- *Controls over the period-end financial reporting process.*
- *Policies that address significant business control and risk management practices.*

14.5 INFORMATION TECHNOLOGY GENERAL CONTROLS (COBIT 5)

IT general controls are controls embedded within IT processes that provide a reliable operating environment and support the effective operation of application controls.

14.5.1 Security Management (APO13)

Management should define, operate and monitor a system for information security management and keep the impact and occurrence of information security incidents within the governmental entity's risk appetite levels. In order to accomplish this, management should:

1) *Establish and maintain an information security management system that provides a standard, formal and continuous approach to security management for information, enabling secure technology and business processes that are aligned with business requirements and governmental entity security management.*

2) *Maintain an information security plan that describes how information security risk is to be managed and aligned with the governmental entity strategy and governmental entity architecture. Ensure that recommendations for implementing security improvements are based on approved business cases and implemented as an integral part of services and solutions development, then operated as an integral part of business operation.*

14.5.2 Logical and Physical Access (DSS05.04 and DSS05.05)

Management should protect governmental entity information to maintain the level of information security risk acceptable to the governmental entity in accordance with the security policy and establish and maintain information security roles and access privileges and perform security monitoring. They should also minimize the business impact of operational information security vulnerabilities and incidents. In order to accomplish this, management should:

1) *Ensure that all users have information access rights in accordance with their business requirements and co-ordinate with business units that manage their own access rights within business processes.*

2) *Define and implement procedures to grant, limit and revoke access to premises, buildings and areas according to business needs, including emergencies. Access to premises, buildings and areas should be justified, authorized, logged and monitored. This should apply to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party.*

14.5.3 Configuration Management (BAI10.01)

Management should establish and maintain a logical model of the services, assets, and infrastructure and how to record configuration items (CIs) and the relationships amongst them. They should include the CIs considered necessary to manage services effectively and to provide a single reliable description of the assets in a service. In order to accomplish this, management should:

1) *Define and agree on the scope and level of detail for configuration management (i.e., which services, assets and infrastructure configurable items to include).*

2) *Establish and maintain a logical model for configuration management, including information on configuration item types, configuration item attributes, relationship types, relationship attributes and status codes.*

14.5.4 Segregation of Duties (APO01.02)

Management should establish, agree on, and communicate roles and responsibilities of IT personnel, as well as other stakeholders with responsibilities for governmental entity IT, that clearly reflect overall business needs and IT objectives and relevant personnel's authority, responsibilities and accountability. In order to accomplish this, management should:

1) *Establish, agree on and communicate IT-related roles and responsibilities for all personnel in the governmental entity, in alignment with business needs and objectives. Clearly delineate responsibilities and accountabilities, especially for decision making and approvals.*

2) *Consider requirements from governmental entity and IT service continuity when defining roles, including staff back-up and cross-training requirements.*

3) *Provide input to the IT service continuity process by maintaining up-to-date contact information and role descriptions in the governmental entity.*

4) *Include in role and responsibility descriptions adherence to management policies and procedures, the code of ethics, and professional practices.*

5) *Implement adequate supervisory practices to ensure that roles and responsibilities are properly exercised, to assess whether all personnel have sufficient authority and resources to execute their roles and responsibilities, and to generally review performance. The level of supervision should be in line with the sensitivity of the position and extent of responsibilities assigned.*

6) *Ensure that accountability is defined through roles and responsibilities.*

7) *Structure roles and responsibilities to reduce the possibility for a single role to compromise a critical process.*

14.5.6 Contingency Planning (DSS04)

Management should establish and maintain a plan to enable the business and IT to respond to incidents and disruptions in order to continue operation of critical business processes and required IT services and maintain availability of information at a level acceptable to the governmental entity. The governmental entity should continue critical business operations and maintain availability of information at a level acceptable to the governmental entity in the event of a significant disruption. In order to accomplish this, management should:

1) *Define business continuity policy and scope aligned with governmental entity and stakeholder objectives.*

2) *Evaluate business continuity management options and choose a cost-effective and viable continuity strategy that will ensure governmental entity recovery and continuity in the face of a disaster or other major incident or disruption.*

3) *Develop a business continuity plan (BCP) based on the strategy that documents the procedures and information in readiness for use in an incident to enable the governmental entity to continue its critical activities.*

4) *Test the continuity arrangements on a regular basis to exercise the recovery plans against predetermined outcomes and to allow innovative solutions to be developed and help to verify over time that the plan will work as anticipated.*

5) *Conduct a management review of the continuity capability at regular intervals to ensure its continued suitability, adequacy and effectiveness. Manage changes to the plan in accordance with the change control process to ensure that the continuity plan is kept up to date and continually reflects actual business requirements.*

6) *Provide all concerned internal and external parties with regular training sessions regarding the procedures and their roles and responsibilities in case of disruption.*

7) *Maintain availability of business-critical information.*

8) *Assess the adequacy of the BCP following the successful resumption of business processes and services after a disruption.*

14.6 APPLICATION CONTROLS (GTAG)

Application controls are those controls that pertain to the scope of individual business processes or application systems, including data edits, separation of business functions, balancing of processing totals, transaction logging, and error reporting. Therefore the objective of application controls is to ensure that:

1) *Input data is accurate, complete, authorized, and correct.*
2) *Data is processed as intended in an acceptable time period.*
3) *Data stored is accurate and complete.*
4) *Outputs are accurate and complete.*
5) *A record is maintained to track the process of data from input to storage and to the eventual output.*

14.6.1 Input Controls

These controls are designed to provide reasonable assurance that data received or computer processing is appropriately authorized and converted into a machine-sensible form and that data is not lost, suppressed, added, duplicated, or improperly changed. Computerized input controls include data checks and validation procedures such as check digits, record counts, hatch totals, and batch financial tools, while computerized edit routines – which are designed to detect data errors – include valid character tests, missing data tests, sequence tests, and limit or reasonableness tests. Domains of input controls include:

1) *Data checks and validation.*

2) *Automated authorization, approval, and override.*
3) *Automated segregation of duties and access rights.*
4) *Pended items.*

14.6.2 File and Data Transmission Controls

These controls ensure that internal and external electronically transmitted files and transactions are received from an identified source and processed accurately and completely. Domains of file and data transmission controls include:

1) *File transmission controls.*
2) *Data transmission controls.*

14.6.3 Processing Controls

Processing controls are designed to provide reasonable assurance that data processing has been performed as intended without any omission or double-counting. Many processing controls are the same as the input controls, particularly for online or real-time processing systems, but are used during the processing phases. These controls include run-to-run totals, control-total reports, and file and operator controls, such as external and internal labels, system logs of computer operations, and limit or reasonableness tests. Domains of processing controls include:

1) *Automated file identification and validation.*
2) *Automated functionality and calculations.*
3) *Audit trails and overrides.*
4) *Data extraction, filtering, and reporting.*
5) *Interface balancing.*
6) *Automated functionality and aging.*
7) *Duplicate checks.*

14.6.4 Output Controls

Output controls are designed to provide reasonable assurance that processing results are accurate and distributed to authorized personnel only. Control totals produced as output during processing should be compared and reconciled to input and run-to-run control totals produced during processing. Computer-generated change reports for master files should be compared to original source documents to assure information is correct. Domains of output controls include:

1) *General ledger posting.*
2) *Sub-ledger posting.*

14.6.5 Master Files and Standing Data Controls

These controls ensure the integrity and accuracy of master files and standing data. Domain of master files and standing data controls includes: update authorization.

14.7 INFORMATION SECURITY FRAMEWORK

The Indiana Office of Technology (IOT) also developed and instituted an Information Security Framework (ISF) that applies to all state agencies supported by IOT. The ISF sets policy, establishes control objectives and controls and references practices that secures Indiana government information assets. The practices referenced in the Information Security Framework can be accessed online at in.gov/iot/2339.htm.

14.8 DOCUMENTATION AND RETENTION

14.8.1 Programming Documentation

During the course of a regularly scheduled audit, documentation must be available to the State Board of Accounts Field Examiners that provides 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 how the computer system processes accounting information.

14.8.2 Operations Documentation

For each computerized accounting system, procedures must be adequately documented to ensure all processing and maintenance is performed. Examples include instructions, checklists, and logs to ensure:

- *Daily, monthly and year-end processes are performed correctly and completely.*
- *Required reports are generated and balanced.*
- *Backups are completed successfully and cycled appropriately.*
- *Virus definitions are updated regularly.*
- *Security patches and upgrades are installed.*

14.8.3 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.

14.8.4 Information Retention and Access

A detailed transaction history (similar to a manually posted ledger page) must be maintained supporting each account. At least the last twelve months of transactions must be accessible on-line. Additional transactional history must be retained back to the date of the last audit. This additional history must be retained on-line or otherwise archived and easily accessible by State Board of Accounts Field Examiners. Records should also be retained in compliance with the appropriate retention schedule as approved by the Indiana Commission on Public Records.

Public records, financial statement information, and supporting information generated through the computer system must be maintained in a manner that will allow access for audit and public inquiry. Acceptable mechanisms include hardcopy, on equipment provided by the governmental unit, or via the Internet.