REPORT NO. 2010-062
DECEMBER 2009

SUMMARY REPORT OF INFORMATION TECHNOLOGY AUDIT FINDINGS

Included In Our Financial and Operational Audit Reports
Issued During the 2008-09 Fiscal Year

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

A listing of the specific entities for which audit reports included information technology (IT) audit findings is included in this report as Exhibit A.

The project was conducted by Hilda S. Morgan, CPA, CISA, and supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CISA, Audit Manager, by e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

This report and other reports prepared by the Auditor General can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 487-9024; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

SUMMARY REPORT OF INFORMATION TECHNOLOGY AUDIT FINDINGS

Included In Our Financial and Operational Audit Reports
Issued During the 2008-09 Fiscal Year

SUMMARY

Public entities rely heavily on information technology (IT) to achieve their missions and business objectives. As such, IT controls are an integral part of entity internal control systems. The Auditor General evaluates the effectiveness of entity controls over IT as a part of financial and operational audits. IT audit findings included in our financial and operational audit reports issued during the 2008-09 fiscal year are summarized below:

- **In 87 audit reports, we disclosed 613 IT audit findings involving 80 public entities. These findings related to entity IT controls that were deficient or needed improvement. Of the 613 IT audit findings, 144 findings, or approximately 23 percent, were also included in audit reports for the same entities from previous fiscal years. Nineteen of the findings had been included in more than one previous audit report for the same entity.**
- **The most prevalent IT audit findings disclosed that improvements were needed in controls over access to entity data and IT resources and described deficiencies in entity IT security management.**
- **The nature and extent of the IT audit findings disclosed in our audits and the percentage of repeated findings are indicative of the need for entity management, those charged with governance, and other stakeholders to place increased emphasis on improving the security and control over data and IT resources.**

BACKGROUND

Information and the related technology are critical public assets. Public entities, including State agencies and institutions of public education, depend on IT to achieve their missions and to record, process, maintain, and report essential financial and program information. However, the widespread use of IT, without proper safeguards, can lead to vulnerabilities that enable the perpetration of errors by employees in their daily work processes and frauds by persons with malicious intentions.

Public entity management, therefore, has an important stewardship responsibility for establishing effective IT controls that provide reasonable assurance of the achievement of management's control objectives, including, in particular, the confidentiality, integrity, and availability of data and IT resources. The absence of effective IT controls can result in significant risks to entity operations and assets, such as risk of unauthorized or erroneous disclosure, modification, or destruction of financial information and IT resources. Examples include:

- Financial resources, such as payments and collections, could be lost or stolen.
- IT resources could be used for unauthorized purposes, including diverting financial resources and launching attacks on other systems or networks.
- Information that is confidential or exempt from public disclosure by law, such as student data, taxpayer data, Social Security numbers, medical records, other personally identifiable information, and proprietary business information could be inappropriately added, disclosed, copied, modified, deleted, or destroyed.
- Critical operations, such as those supporting law enforcement and emergency services, could be disrupted.

- Information could be modified for purposes such as identity theft, embezzlement, and other types of crime.
- Public confidence in State government and the public education system could be diminished as a result of embarrassing incidents such as the disclosure of personally identifiable information, unavailable or poorly functioning IT-dependent services, IT-related fraud, or costly mismanagement of large IT system acquisition or development projects.

Recognizing the need for improved IT security management in State government, the Florida Legislature has enacted recent legislation (Chapter 2009-80, Laws of Florida) that provides for additional IT security management and reporting responsibilities for the Agency for Enterprise Information Technology (AEIT) and other State agencies as defined in Section 216.011(1)(qq), Florida Statutes. This legislation provides, in part, that:

- The Office of Information Security (Office) is established within the Agency for Enterprise Information Technology, to be overseen by a state Chief Information Security Officer.
- The Office is responsible for establishing rules and publishing guidelines for ensuring an appropriate level of security for all data and IT resources for executive branch agencies.
- The Office is required to develop, and annually update by February 1, an enterprise information security strategic plan.
- The Office is required to submit to the Governor, President of the Senate, and Speaker of the House of Representatives by December 31, 2010, a proposed implementation plan for IT security.
- State agencies are required to annually submit to the Office strategic and operational security plans pursuant to the rules and guidelines established by the Office.

Similar provisions of law do not exist for institutions of public education.

SUMMARY OF IT AUDIT FINDINGS

The Auditor General conducts financial and operational audits of State agencies, universities, community colleges, district school boards, and other governmental entities pursuant to Section 11.45(2), Florida Statutes. The Auditor General may, pursuant to Section 11.45(3), Florida Statutes, conduct audits or other engagements of the accounts, records, and IT programs, activities, functions, or systems of any governmental entity created or established by law.

We evaluate IT controls in financial audits and in many operational audits. Consideration of IT controls is an essential and significant part of the audit process in these audits because entity business processes that are relevant to the audit objectives are generally dependent on IT. In addition, IT systems are the specific topic of many operational audits by our IT Audits Division.

During the 2008-09 fiscal year, we issued 219 audit reports, including 167 financial or operational audit reports. Of the 167 financial or operational audit reports, 87 reports (representing 80 entities) included one or more findings relating to entity management and control of IT, for a total of 613 findings. Of the 613 IT audit findings, 144 findings, or approximately 23 percent, were also included in audit reports for the same entities from previous fiscal years. Nineteen of the findings had been included in more than one previous audit report for the same entity.

We have analyzed each of the 613 IT audit findings and, for the purposes of this report, summarized the findings into nine control categories based on the Federal Information System Controls Audit Manual (FISCAM), issued by the United States Government Accountability Office (GAO) in February 2009. The nine control categories, representing a grouping of related controls having similar types of risks, are:

General Controls

- Security Management: Controls providing assurance that security management is effective. Examples include a security management program, periodic risk assessments and validation, and security control policies and procedures.
- Access Controls: Controls providing assurance that access to data, software, equipment, and facilities is reasonable and restricted to authorized individuals.
- Configuration Management: Controls providing assurance that changes to IT system resources are authorized and systems are configured and operated securely and as intended.
- Separation of Duties: Controls providing assurance that incompatible duties are effectively separated.
- Contingency Planning: Controls protecting information resources, minimizing the risk of unplanned interruptions, and providing for the recovery of critical operations should interruptions occur.

Business Process Application Controls

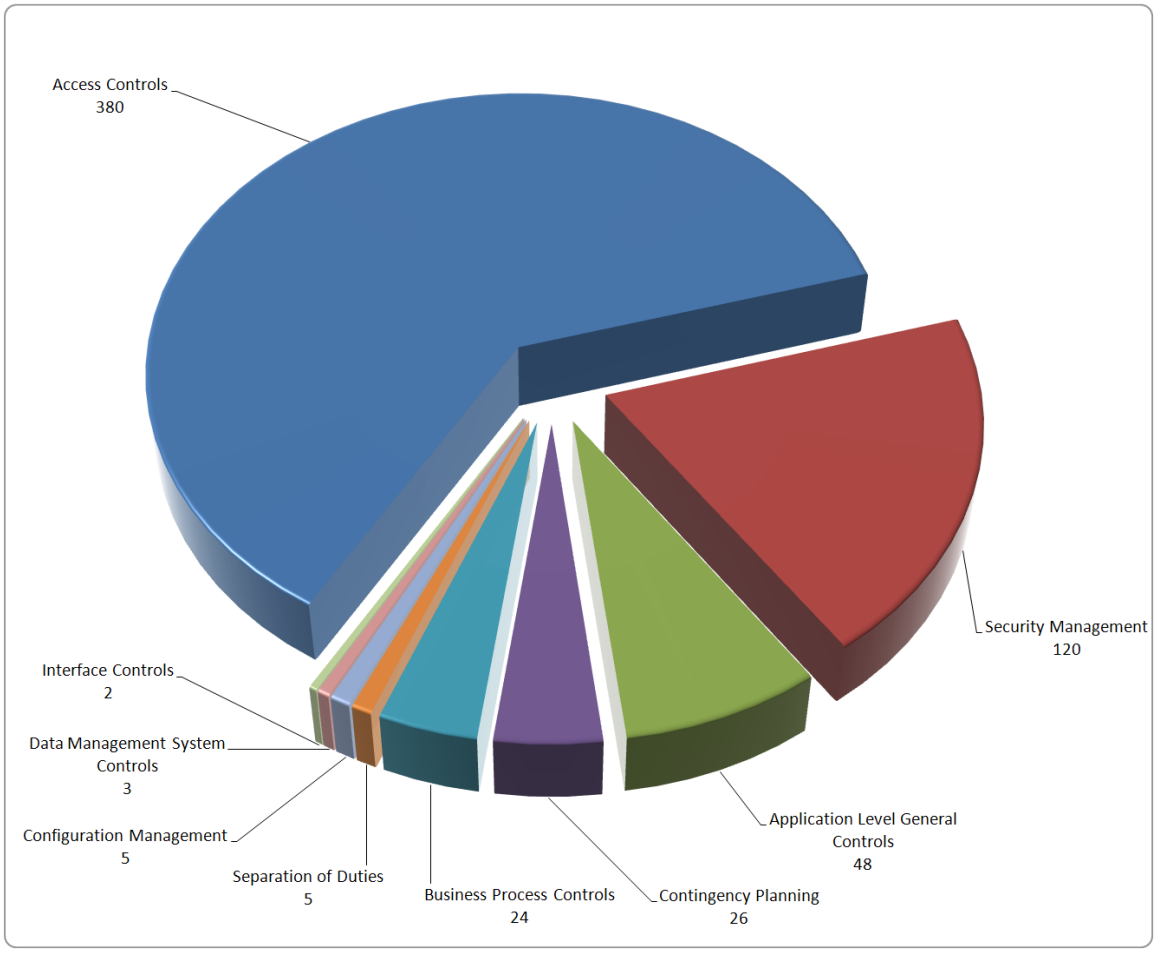
- Application Level General Controls: General controls, including the five types of controls listed above, operating at the business process application level.
- Business Process Controls: Automated and manual controls applied to business process flows, including controls over transaction data input, processing, and output and controls over master data.
- Interface Controls: Controls over the timely, accurate, and complete processing of information between applications and other feeder and receiving systems and the complete and accurate migration of clean data during conversion.
- Data Management System Controls: Controls used in data management systems, such as database management systems, middleware, data warehouse software, and data extraction and reporting software.

The IT controls included within the scope of individual audits varied based on many factors, including the overall audit objectives and scope, the nature of entity business operations and the entity's use of IT, the entity's IT environment and other risk-based planning considerations. Controls such as Access Controls and Security Management were frequently selected for audit. In contrast, other IT controls such as Interface Controls were not as frequently included in the scope of audits. Consequently, any conclusions drawn based on the distribution of IT audit findings among the nine control categories should take into consideration that certain IT controls were addressed in audits more frequently than other IT controls.

The following table and chart provide a high-level summary of IT audit findings by control category (for a more detailed breakdown and description of the findings, please see Exhibit B of this report):

Control Category	Number of Findings
Access Controls	380
Security Management	120
Application Level General Controls	48
Contingency Planning	26
Business Process Controls	24
Separation of Duties	5
Configuration Management	5
Data Management System Controls	3
Interface Controls	2
Total Number of Findings	**613**

Number of Findings By Control Category



As shown above, the predominant IT audit findings were in the categories of Access Controls and Security Management. Although these categories of IT controls were frequently included within the scope of the 87 audits, the number of findings in these two categories indicates that many opportunities exist within State government and the public education system for improving IT security, as discussed below.

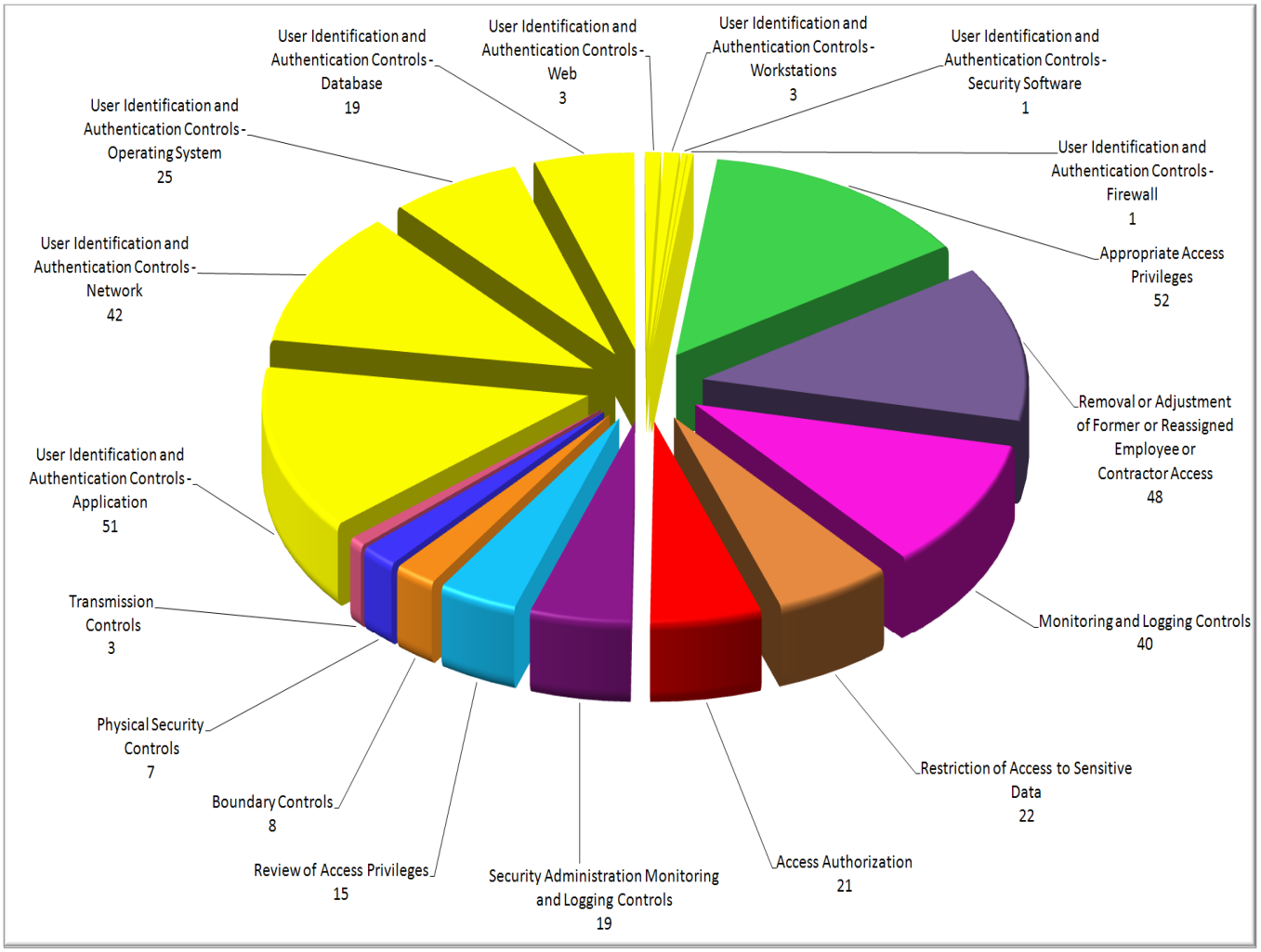
Access Control Findings

Access controls limit or detect inappropriate access to IT resources, thereby protecting the IT resources from unauthorized disclosure, modification, and loss. Without adequate access controls, unauthorized individuals, including outside intruders and former employees, can surreptitiously read and copy sensitive data and make undetected changes or deletions for malicious purposes or personal gain. In addition, authorized users can intentionally or unintentionally read, add, modify, delete, or exfiltrate (remove) data or execute changes that are outside their span of authority.

The following table and chart provide a breakdown of access control findings by the specific control technique needing improvement.

Access Controls – Control Techniques	Number of Findings	Number of Entities
Appropriate Access Privileges	52	45
User Identification and Authentication Controls – Application	51	44
Removal or Adjustment of Former or Reassigned Employee or Contractor Access	48	41
User Identification and Authentication Controls – Network	42	41
Monitoring and Logging Controls	40	28
User Identification and Authentication Controls - Operating System	25	25
Restriction of Access to Sensitive Data	22	20
Access Authorization	21	17
User Identification and Authentication Controls – Database	19	16
Security Administration Monitoring and Logging Controls	19	18
Review of Access Privileges	15	13
Boundary Controls	8	8
Physical Security Controls	7	6
Transmission Controls	3	3
User Identification and Authentication Controls - Web	3	3
User Identification and Authentication Controls - Workstations	3	3
User Identification and Authentication Controls - Security Software	1	1
User Identification and Authentication Controls - Firewall	1	1
Total Number of Findings	**380**	

Access Controls
Number of Findings By Control Technique



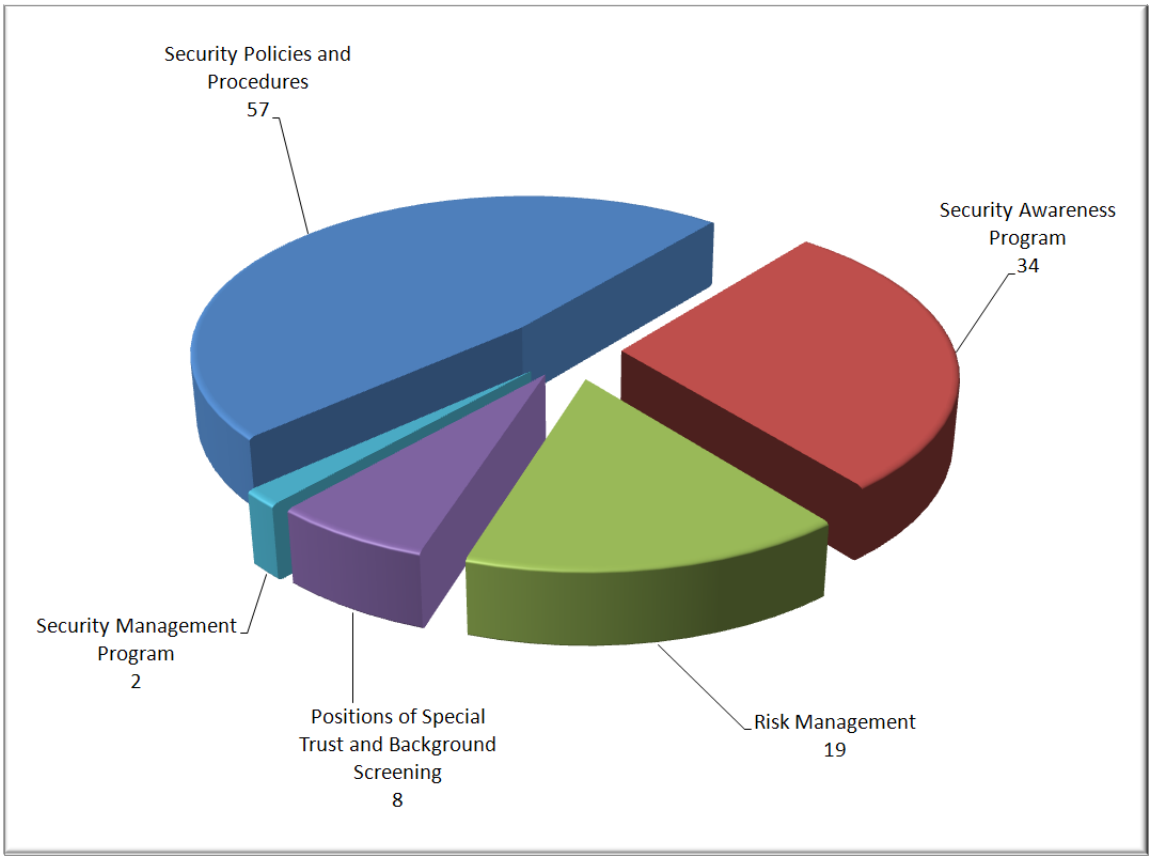
Security Management Findings

The effectiveness of an entity's access controls and other aspects of IT security are dependent in part on the effectiveness of its overall security management. An entitywide security management program is the foundation of a security control structure and a reflection of senior management's commitment to addressing security risks. The security management program should establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of the procedures. Improvements in the overall IT security management of public entities would enhance their ability to identify, assess, and remedy deficiencies in IT security controls in a cost-effective manner.

The following table and chart provide a breakdown of security management findings by the specific control technique needing improvement.

Security Management – Control Techniques	Number of Findings	Number of Entities
Security Policies and Procedures	57	48
Security Awareness Program	34	33
Risk Management	19	17
Positions of Special Trust and Background Screening	8	8
Security Management Program	2	1
Total Number of Findings	**120**	

Security Management
Number of Findings By Control Technique

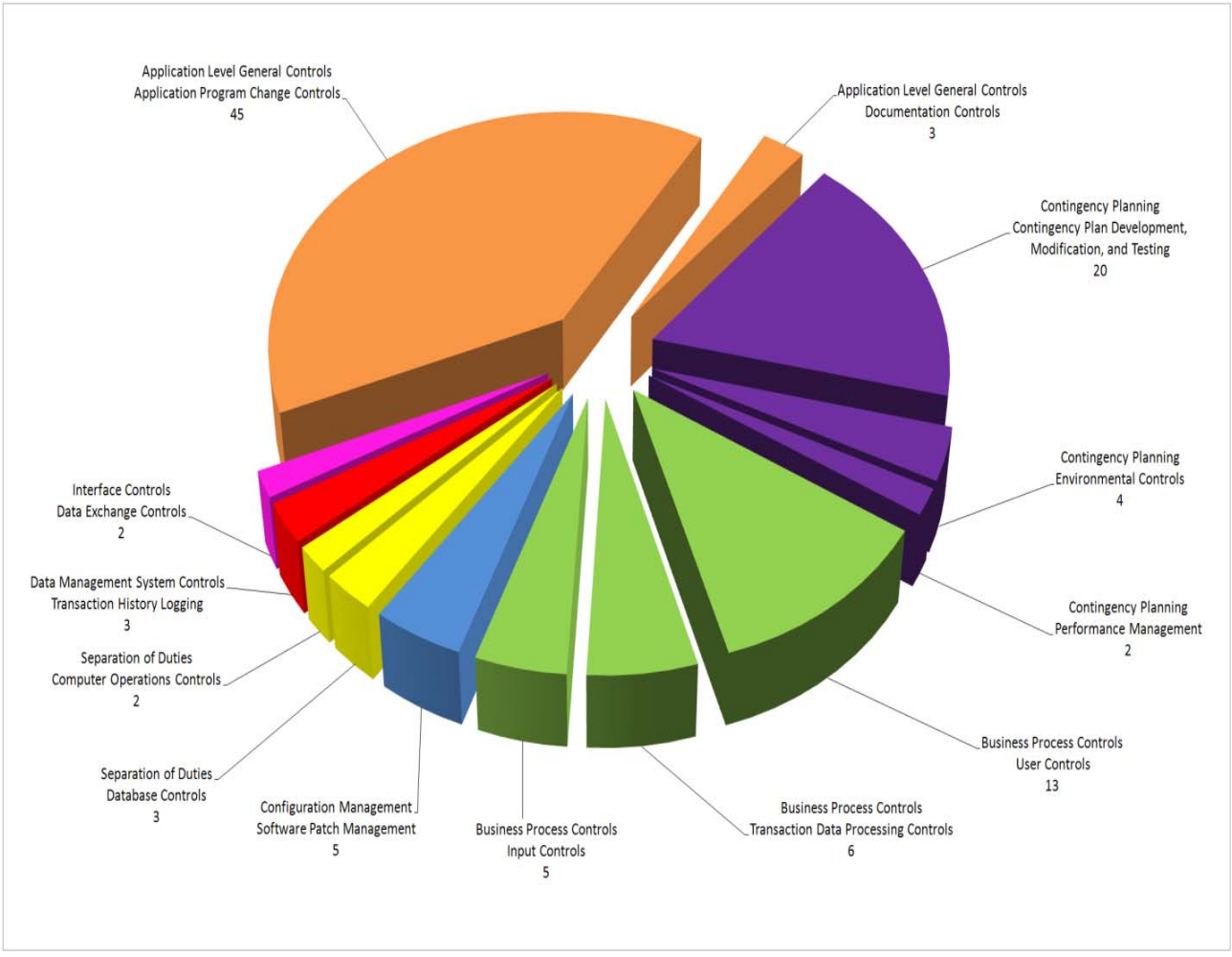


Other Control Categories

The following table and charts provide a breakdown of IT audit findings that were grouped into the seven other control categories, including the specific control techniques that were the subject of the findings.

Control Category	Control Technique	Number of Findings	Number of Entities
Application Level General Controls	Application Program Change Controls	45	28
	Documentation Controls	3	2
Contingency Planning	Contingency Plan Development, Modification, and Testing	20	20
	Environmental Controls	4	4
	Performance Management	2	2
Business Process Controls	User Controls	13	9
	Transaction Data Processing Controls	6	5
	Input Controls	5	4
Configuration Management	Software Patch Management	5	5
Separation of Duties	Database Controls	3	3
	Computer Operations Controls	2	2
Data Management System Controls	Transaction History Logging	3	3
Interface Controls	Data Exchange Controls	2	2
Total Number of Findings		**113**	

Number of Findings By Control Category and Control Technique



RECOMMENDATION FOR THE LEGISLATURE

Maintaining effective internal controls, including IT controls, is an important management responsibility. As shown in the summarizations of IT control issues provided above, the nature and extent of IT audit findings noted in our audit reports issued during the 2008-09 fiscal year and the percentage of repeated findings indicate that information security programs have not yet been fully or effectively implemented for numerous entities and that entity management, those charged with governance, and other stakeholders should place an increased emphasis on improving the security and control of public data and IT resources. Without effective IT security and control practices, controls may continue to be inadequate; responsibilities may be unclear, misunderstood, or improperly implemented; and controls may be inconsistently applied.

As previously discussed, Chapter 2009-80, Laws of Florida, provides that the Office of Information Security within AEIT is responsible for establishing rules and publishing guidelines for ensuring an appropriate level of security for data and IT resources for executive branch agencies. In addition, Section 282.318(4), Florida Statutes, provides that each agency head is responsible for assisting the Office by, in part, conducting and updating comprehensive security risk analyses, establishing written internal policies and procedures, developing cost-effective safeguards to reduce identified security risks, and ensuring the conduct of periodic internal audits and evaluations of agency security programs for data, information, and IT resources. Consistent with these requirements, we encourage agency management, those charged with governance, and other stakeholders to work toward improving IT security and control practices.

Similar provisions do not exist in State law for promoting and encouraging effective IT security and control in Florida's K-20 education system. Some administrative rules and regulations exist that address certain IT security requirements for educational entities. However, State law does not clearly address responsibilities within the public education system for the security and control of data and IT resources.

Of the 80 entities for which audit reports were released in the 2008-09 fiscal year disclosing IT audit findings, 56 were educational entities. The significant number of educational entities with IT audit findings, the importance of IT to the accomplishment of educational entity missions, and the existence of significant confidential and exempt information within educational entity IT systems indicates a need to promote and encourage IT security and control practices in the public education system.

Identifying and addressing responsibilities within Florida's K-20 public education system for the security and control of data and IT resources is a significant task. Florida's K–20 public education system consists of a diverse group of entities, including the State University System, the State college system, and district school boards, as well as other related entities such as Florida Distance Learning and the Florida Center for Library Automation. These educational entities have different missions, governance structures, requirements, and levels of resources. These entities all use IT resources to various degrees; however, the IT environments vary from entity to entity in such areas as the type of IT infrastructure, type and number of application systems, age of the infrastructure and systems, size of the entity being supported, and the number and qualifications of staff and amount of monetary resources available to support IT. Financial application systems used by educational entities range from complex Enterprise Resource Planning systems to legacy mainframe systems. Many educational entities use IT consortia, regional data centers, or private service providers for various levels of IT services.

Because of the diverse and complex nature of the educational entities' environments, a collaborative approach is necessary to identify strategies and solutions for achieving an appropriate level of security of data and IT resources among all educational entities while at the same time allowing these entities the autonomy provided for in State Constitution and law. Within the governance structure for Florida's K-20 public education system, there are organizations that may be able to assist entities within their jurisdiction. Such organizations include the Department of Education that has certain oversight responsibilities for school districts and colleges; the Information Resource Management office within the State University System Board of Governors that has issued a regulation for Universities regarding security of data and related IT resources; and the Chief Information Officers (CIOs) of educational entities, who collaborate and share information regarding the advancement of educational technology. In addition, AEIT is well positioned to provide information and assistance to all public entities regarding IT security and control best practices.

Recommendation: We recommend that the Legislature consider establishing a workgroup composed of applicable stakeholders to study and make recommendations for strategies to promote an appropriate level of security of data and IT resources for Florida's educational entities. The workgroup should include representatives from the Department of Education, the Board of Governors of the State University System, the educational entities' CIO communities, and AEIT. Matters to be addressed by the workgroup could include strategies in the following areas: promoting information security awareness, standards, and guidelines; conducting security planning and risk analyses; establishing cost-effective IT security and control practices to reduce identified security risks; and ensuring the conduct of periodic internal audits and evaluations of information security programs. The workgroup should consider establishing a long-range security plan for achieving an appropriate level of security of data and IT resources for Florida's K-20 education system.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objective of this project was to analyze and summarize all IT audit findings reported by the Auditor General during the 2008-09 fiscal year.

The scope of this project included a review of 167 Auditor General financial or operational audit reports released during the 2008-09 fiscal year.

Our methodology included a review of applicable audit reports and an analysis and summarization of IT audit findings. We conducted this review in accordance with applicable generally accepted government auditing standards. We believe that the procedures performed provide a reasonable basis for the summaries of IT audit findings included in this report.

AUTHORITY

Pursuant to the provisions of Section 11.45(3)(b), Florida Statutes, I have directed that this report be prepared to present a summary of IT audit findings included in our financial and operational audit reports issued during the 2008-09 fiscal year.

David W. Martin, CPA
Auditor General

EXHIBIT - A

LISTING OF FINANCIAL AND OPERATIONAL AUDIT REPORTS ISSUED DURING THE 2008-09 FISCAL YEAR THAT INCLUDED INFORMATION TECHNOLOGY (IT) AUDIT FINDINGS

Report No.	Entity Name
2009-003	Agency for Workforce Innovation
2009-004	Department of Financial Services
2009-011	Department of Corrections
2009-013	Department of Citrus
2009-017	Department of Transportation
2009-018	Department of Health
2009-020	Department of Legal Affairs
2009-022	Pasco-Hernando Community College
2009-024	Department of Revenue
2009-028	Marion County District School Board
2009-029	Escambia County District School Board
2009-031	Department of State
2009-032	Office of Insurance Regulation
2009-033	Palm Beach Community College
2009-034	Hernando County District School Board
2009-036	Office of Insurance Regulation
2009-038	Department of Law Enforcement
2009-039	Department of Children and Family Services
2009-040	Indian River County District School Board
2009-041	Santa Fe College
2009-048	Lee County District School Board
2009-049	Department of State
2009-052	Department of Management Services
2009-053	Department of Financial Services
2009-055	Seminole County District School Board
2009-056	Madison County District School Board
2009-057	St. Petersburg College
2009-062	Gulf Coast Community College
2009-063	Nassau County District School Board
2009-065	Columbia County District School Board
2009-067	Lake County District School Board
2009-070	Agency for Workforce Innovation, Department of Revenue, and Department of Management Services
2009-078	Department of Management Services, Division of Administrative Hearings, Florida Commission on Human Relations, and Public Employees Relations Commission
2009-082	Gulf County District School Board
2009-083	Agency for Workforce Innovation, Department of Agriculture and Consumer Services, Department of Health, Fish and Wildlife Conservation Commission, and Office of State Courts Administrator
2009-086	Division of Emergency Management
2009-087	Florida Agricultural and Mechanical University
2009-091	Department of Financial Services
2009-093	Department of Transportation
2009-094	Jefferson County District School Board
2009-096	Sumter County District School Board
2009-097	Gilchrist County District School Board
2009-098	Hardee County District School Board
2009-099	Baker County District School Board
2009-100	Department of Children and Family Services
2009-101	Department of the Lottery
2009-102	Citizens Property Insurance Corporation
2009-109	University of West Florida
2009-118	Jackson County District School Board
2009-119	Suwannee County District School Board
2009-128	Liberty County District School Board
2009-131	Northwest Florida State College
2009-132	North Florida Community College
2009-134	Dixie County District School Board
2009-138	Franklin County District School Board
2009-139	Levy County District School Board
2009-140	Hamilton County District School Board
2009-141A	Citrus County District School Board
2009-142	Hendry County District School Board
2009-143	Holmes County District School Board
2009-144	Department of Financial Services, Department of Community Affairs, Agency for Workforce Innovation, Department of Revenue, Department of Education, Department of Health, Department of Children and Family Services, and Division of Emergency Management
2009-145	Lake-Sumter Community College
2009-149	Valencia Community College
2009-151	Miami Dade College
2009-152	Bay County District School Board
2009-153	Bradford County District School Board
2009-154	Walton County District School Board
2009-155	Indian River State College
2009-159	Polk Community College
2009-161	Santa Rosa County District School Board
2009-163	Washington County District School Board
2009-164	Wakulla County District School Board
2009-166	Glades County District School Board
2009-169	Putnam County District School Board
2009-171	Taylor County District School Board
2009-172	Clay County District School Board
2009-175	Highlands County District School Board
2009-179	Charlotte County District School Board
2009-186	Pinellas County District School Board
2009-188	Gadsden County District School Board
2009-189	Leon County District School Board
2009-197	Department of Veterans' Affairs
2009-199	Department of Revenue
2009-200	Department of Management Services
2009-208	Department of Education
2009-209	Monroe County District School Board
2009-213	Department of Education

EXHIBIT B

SUMMARY OF IT AUDIT FINDINGS
BY CONTROL CATEGORY AND TECHNIQUE

Control Category	Control Technique	Description	Finding Results and Issues	No. of Findings	No. of State Agencies[1]	No. of Educational Entities	Total No. of Entities
1. Security Management	1. Security Management Program	Senior management should establish a security management structure for entitywide, system, and application levels that have adequate independence, authority, expertise, and resources. An information systems security manager should be appointed at an agency (entity) level and at appropriate subordinate (i.e., system and application) levels and given appropriate authority. The security program documentation should clearly identify owners of computer-related resources and those responsible for managing access to computer resources. Security responsibilities and expected behaviors should be clearly defined at the entitywide, system, and application levels for information resource owners and users, information technology management and staff, senior management, and security administrators.	▪ The placement of the CIO within the Department's organizational structure needed review and the scope of his authority for performing IT duties assigned in State law needed improvement to provide increased oversight of all Department IT functions. ▪ The Department and Divisions had not clearly established the roles and responsibilities of the Department's information security manager and the Division data security administrators.	2	1	0	1
Security Management	2. Risk Management	Appropriate risk assessment policies and procedures should be documented and based on security categorizations. Information systems should be categorized based on the potential impact that the loss of confidentiality, integrity, or availability would have on operations, assets, or individuals. Risks should be reassessed for the entitywide, system, and application levels on a periodic basis or whenever systems, applications, facilities, or other conditions change. Risk assessment documentation should include security plans, risk assessments, security test and evaluation results, and appropriate management approvals. Changes to systems, facilities, or other conditions and identified security vulnerabilities should be analyzed to determine their impact on risk and the risk assessment should be performed or revised as necessary.	▪ There were no policies and procedures for a periodic risk analysis for critical information resources or for a comprehensive risk analysis after major changes in software, procedures, environment, organization, or hardware. ▪ A formal risk assessment had not been performed to identify and document information technology systems and resources, vulnerabilities and exposures, policies and control measures, and management's signed acceptance of unmitigated risks. ▪ The auditee did not conduct routine network and system vulnerability testing. ▪ There was no enterprise risk management function, consequently there was no documentation to support that an enterprise-wide evaluation of the effectiveness of controls had been conducted. ▪ Contrary to the security policy, the auditee did not have an approved security plan for a major information system. ▪ Contrary to the security policy, the auditee did not perform a certification and accreditation for a major information system. ▪ The first phase of a strategic plan had been completed but still lacked further exposure to IT stakeholders and formal approval. ▪ Vulnerability assessment and penetration testing had never been performed.	19	6	11	17

[1] For the purposes of this summary, Citizens Property Insurance Corporation was included with the State agencies.

EXHIBIT B (Continued)

SUMMARY OF IT AUDIT FINDINGS
BY CONTROL CATEGORY AND TECHNIQUE

Control Category	Control Technique	Description	Finding Results and Issues	No. of Findings	No. of State Agencies	No. of Educational Entities	Total No. of Entities
			▪ The auditee did not have a policy for the classification of data according to risk and importance to support decisions regarding the appropriate level of data protection to be employed during systems development and change activities. ▪ The auditee had not classified its data according to sensitivity or level of significance. ▪ Data owners had not been identified. ▪ The Department had not prepared security plans and strategies for implementing appropriate cost-effective safeguards to reduce, eliminate, or recover from the identified risks to data, information, and IT resources.				
Security Management	3. Security Policies and Procedures	Security control policies and procedures at all levels should: ▪ be documented ▪ appropriately consider risk ▪ address purpose, scope, roles, responsibilities, and compliance ▪ ensure that users can be held accountable for their actions ▪ appropriately consider general and application controls ▪ be approved by management ▪ be periodically reviewed and updated. Security policy is senior management's directives to create a computer security program, establish its goals, and assign responsibilities. Procedures are detailed steps to be followed to accomplish particular security-related tasks (for example, preparing new user accounts and assigning the appropriate privileges).	▪ The auditee's Electronic Security for Public Records Policy was outdated. ▪ The auditee lacked written policies and procedures for certain IT functions (including security functions) or they were not sufficiently comprehensive or fully approved. ▪ The auditee did not have written security administration policies and procedures for an application. ▪ There was no written policy prohibiting the sharing of user and system administrator identifications. ▪ There were no written policies to prohibit the granting of workstation administrator rights to end-users. ▪ There were no written procedures for requesting, approving, assigning, and removing user access privileges. ▪ There were no written procedures addressing the erasure, data backup, or physical security of surplus IT property. ▪ The auditee did not follow its written property disposal procedures. ▪ The auditee had not established security protocols for controlling access through user names and passwords. ▪ The auditee had not established a process to ascertain the appropriateness of security controls for their vendor-owned application. ▪ There were no policies and procedures for monitoring access privileges to the application or the security events were not monitored. ▪ The auditee allowed the use of instant messaging software on its computers without establishing a specific policy or procedures governing its secure use. ▪ There were no written policies and procedures for network and system administration functions such as configuration and management of routers, switches, and other security devices. ▪ No written policies and procedures	57	12	36	48

EXHIBIT B (Continued)

SUMMARY OF IT AUDIT FINDINGS
BY CONTROL CATEGORY AND TECHNIQUE

Control Category	Control Technique	Description	Finding Results and Issues	No. of Findings	No. of State Agencies	No. of Educational Entities	Total No. of Entities
			existed for backup, recovery, and tape rotation of application data and programs. ▪ No written procedures existed for the security monitoring activities of the security administrator. ▪ The Department's security program, including its security policies and procedures, needed improvement. ▪ The Department, nor the divisions, had written procedures in place addressing physical security for the server rooms.				
Security Management	4. Security Awareness Program	An ongoing security awareness program should be implemented that includes security briefings and training that is monitored for all employees with system access and security responsibilities. Training should be documented and monitored. Typical means for establishing and maintaining security awareness include: ▪ informing users of the importance of the information they handle and the legal and business reasons for maintaining its integrity and confidentiality ▪ distributing documentation describing security policies, procedures, and users' responsibilities, including their expected behavior ▪ requiring users to periodically sign a statement acknowledging their awareness and acceptance of responsibility for security and their responsibilities for following all organizational policies ▪ requiring comprehensive security orientation, training, and periodic refresher programs to communicate security guidelines to both new and existing employees and contractors.	▪ The auditee had not developed a written security awareness training program or performed ongoing information technology security awareness training for all employees. ▪ The personnel file did not always include signed Acceptable Use of Information Technology Agreements and the personnel file did not always include a signed Confidentiality and Non-Disclosure Agreement. ▪ The auditee's security awareness training program needed improvement. ▪ Security awareness training was not provided on a recurring basis. ▪ The Department did not retain documentation of employee participation in security awareness training activities.	34	6	27	33
Security Management	5. Positions of Special Trust and Background Screening	For prospective employees, references should be checked and background checks performed. Nondisclosure or security access agreements should be required for employees and contractors assigned to work with sensitive information.	▪ The auditee had not established a written policy for designating positions of special trust. ▪ The auditee had not performed level 2 background screenings with fingerprints for all employees or contractors in positions of special trust. ▪ The auditee's contract for application services did not require that appropriate background screenings be conducted of contractor staff and adequate background checks were not performed for all contracted staff. ▪ The auditee had not identified which positions require access to confidential data or designated those positions as positions of special trust. ▪ The Department did not perform Federal background checks on one	8	8	0	8

EXHIBIT B (Continued)

SUMMARY OF IT AUDIT FINDINGS
BY CONTROL CATEGORY AND TECHNIQUE

Control Category	Control Technique	Description	Finding Results and Issues	No. of Findings	No. of State Agencies	No. of Educational Entities	Total No. of Entities
			division's application contractors. ▪ Department policies contained inconsistent guidance regarding whether contractors could be considered as occupying positions of special trust.				
2. Access Controls	1. Boundary Controls	Networks should be appropriately configured to adequately protect access paths within and between systems, using appropriate technological controls (e.g., routers, firewalls, etc.).	▪ Changes to firewall settings were not monitored. ▪ The auditee was unable to provide documentation of an approved baseline firewall configuration. ▪ The auditee had not installed a firewall to protect its network. ▪ An unauthorized wireless network was in use at the auditee's headquarters even though they monitored for rogue wireless devices. ▪ Default port settings had not been changed where necessary. ▪ There were no written policies and procedures for the use of firewalls. ▪ There was no written procedure to periodically review facilities for rogue wireless access points. ▪ Numerous wireless access points did not have the appropriate firmware.	8	4	4	8
Access Controls	2. User Identification (ID) and Authentication Controls - Application	Users or processes should be appropriately identified and authenticated through logical access controls. User authentication establishes the validity of a user's claimed identity typically during access to a system or application. Logical controls should be designed to restrict legitimate users to the specific systems, programs, and files that they need and prevent others, such as hackers, from entering the system at all. Passwords are the most widely used means of authentication. Controls for protecting the confidentiality of passwords include: ▪ Individual users are uniquely identified rather than sharing group IDs. ▪ Generic user IDs and passwords are not used. ▪ Password selection is controlled by the user and is not subject to disclosure. ▪ Passwords are changed periodically, about every 30 days. ▪ Passwords are not displayed when entered. ▪ Passwords contain alphanumeric and special characters. ▪ Passwords have a minimum character length of at least 8 characters. ▪ Use of old passwords is prohibited. ▪ Vendor-supplied passwords are replaced immediately. ▪ Attempts to log on with invalid passwords are limited.	These findings were for numerous types of applications, including financial, payroll/human resource, student, and others. In some cases, these weaknesses existed for more than one application for an auditee. Application passwords and user IDs: ▪ Passwords were not required to log on to the application. ▪ User IDs and passwords were shared. ▪ Passwords were assigned by the security administrator and could not be changed by the user. ▪ Users were not required to change the password at initial logon. ▪ Password and logon controls did not enforce a password change interval or the interval was too long. ▪ Password and logon controls did not enforce password complexity requirements. ▪ Password and logon controls did not enforce password minimum length requirements or the minimum length was too short. ▪ Password and logon controls did not enforce password reuse rules (history) or the history setting was too short. ▪ Password and logon controls did not limit the number of allowed invalid access attempts or the limitation was too high. ▪ Password and logon controls did not enforce a password-protected timeout for idle workstations or the time set was too long. ▪ There were no password reset	51	17	27	44

EXHIBIT B (Continued)

SUMMARY OF IT AUDIT FINDINGS
BY CONTROL CATEGORY AND TECHNIQUE

Control Category	Control Technique	Description	Finding Results and Issues	No. of Findings	No. of State Agencies	No. of Educational Entities	Total No. of Entities
			procedures for the security software. ▪ Accounts locked after three failed logon attempts were automatically unlocked at midnight. ▪ Users were automatically logged off the system after 120 minutes of inactivity instead of 30. ▪ The default superuser ID was not fully secured. ▪ Password age was set at 0 days.				
Access Controls	3. User ID and Authentication Controls - Database	Same description as shown above for User Identification (ID) and Authentication Controls - Application.	Database passwords and user IDs: ▪ Password standards were not enforced. ▪ User IDs and passwords were shared for administering the database. ▪ Users were not required to change the password at initial logon. ▪ Password and logon controls did not enforce a password change interval or the interval was too long. ▪ Password and logon controls did not enforce password complexity requirements. ▪ Password and logon controls did not enforce password minimum length requirements or the minimum length was too short. ▪ Password and logon controls did not enforce password reuse rules (history) or the history setting was too short. ▪ Password and logon controls did not limit the number of allowed invalid access attempts, the limitation was set too high, or the user could bypass the control by using another session. ▪ Password and logon controls did not enforce a password-protected timeout for databases or the time set was too long. ▪ Vendor default accounts had not been changed.	19	4	12	16
Access Controls	4. User ID and Authentication Controls - Firewall	Same description as shown above for User Identification (ID) and Authentication Controls - Application.	Firewall passwords and user IDs: ▪ User IDs and passwords were shared for administering the firewall. ▪ Passwords did not expire, contrary to procedures.	1	1	0	1
Access Controls	5. User ID and Authentication Controls - Network	Same description as shown above for User Identification (ID) and Authentication Controls - Application.	Network passwords and user IDs: ▪ The network was not password protected. ▪ The password procedures were inconsistent. ▪ There were no password reset procedures for the network. ▪ Network passwords were not required to be changed upon initial logon. ▪ Password and logon controls did not enforce a password change interval or the interval was too long. ▪ Password and logon controls did not enforce password complexity requirements.	42	7	34	41

EXHIBIT B (Continued)

SUMMARY OF IT AUDIT FINDINGS
BY CONTROL CATEGORY AND TECHNIQUE

Control Category	Control Technique	Description	Finding Results and Issues	No. of Findings	No. of State Agencies	No. of Educational Entities	Total No. of Entities
			▪ Password and logon controls did not enforce password minimum length requirements or the minimum length was too short. ▪ Password and logon controls did not enforce password reuse rules (history) or the history setting was too short. ▪ Password and logon controls did not limit the number of allowed invalid access attempts or the limitation was set too high. ▪ Password and logon controls did not enforce a password-protected timeout for the network or the time set was too long. ▪ Local logons were used instead of managed network logons. ▪ The session lock function had not been activated leaving users in control of setting or disabling the session lock function. ▪ The Division still needed to improve the authentication of FTP servers. ▪ Minimum password age was incorrectly set.				
Access Controls	6. User ID and Authentication Controls - Operating System	Same description as shown above for User Identification (ID) and Authentication Controls - Application.	Operating system passwords and user IDs: ▪ No password standards were enforced on the operating system. ▪ Security features had not been configured for the operating system and any user could change their user identifier to a superuser. ▪ Users were not required to change the password at initial logon. ▪ Password and logon controls did not enforce a password change interval or the interval was too long. ▪ Password and logon controls did not enforce password complexity requirements. ▪ Password and logon controls did not enforce password minimum length requirements or the minimum length was too short. ▪ Password and logon controls did not enforce password reuse rules (history) or the history setting was too short. ▪ Password and logon controls did not limit the number of allowed invalid access attempts or the limitation was set too high. ▪ Password and logon controls did not enforce a password-protected timeout for operating systems or the time set was too long. ▪ Vendor default settings had not been changed for the servers. ▪ The default password parameters for some user accounts on production servers were overwritten to make them less restrictive. ▪ The root account and some user	25	1	24	25

EXHIBIT B (Continued)

SUMMARY OF IT AUDIT FINDINGS
BY CONTROL CATEGORY AND TECHNIQUE

Control Category	Control Technique	Description	Finding Results and Issues	No. of Findings	No. of State Agencies	No. of Educational Entities	Total No. of Entities
			accounts on some production servers were set to never expire. ▪ Some operating system user IDs were shared among multiple users.				
Access Controls	7. User ID and Authentication Controls - Security Software	Same description as shown above for User Identification (ID) and Authentication Controls - Application.	Security software passwords and user IDs: ▪ Password and logon controls did not enforce a password change interval or the interval was too long.	1	0	1	1
Access Controls	8. User ID and Authentication Controls - Web	Same description as shown above for User Identification (ID) and Authentication Controls - Application.	Web interface passwords and user IDs: ▪ Password and logon controls did not enforce a password change interval or the interval was too long. ▪ Password and logon controls did not enforce password complexity requirements. ▪ Password and logon controls did not enforce password reuse rules (history) or the history setting was too short. ▪ User IDs and passwords were shared among staff for the Web interface. ▪ The limitation on invalid logon attempts was set too high and automatically reset after 15 minutes. ▪ The automatic inactivity timeout was set at eight hours.	3	3	0	3
Access Controls	9. User ID and Authentication Controls - Workstations	Same description as shown above for User Identification (ID) and Authentication Controls - Application.	Workstation passwords and user IDs: ▪ Password and logon controls did not enforce a password change interval or the interval was too long. ▪ Password and logon controls did not enforce password complexity requirements. ▪ Password and logon controls did not enforce password minimum length requirements or the minimum length was too short. ▪ Password and logon controls did not enforce password reuse rules (history) or the history setting was too short. ▪ Password and logon controls did not limit the number of allowed invalid access attempts on the workstations, the limitation was set too high, or the control could be bypassed. ▪ Password and logon controls could be changed or totally disabled by the user for the password-protected screen-savers on workstations.	3	1	2	3
Access Controls	10. Access Authorization	To adequately control user accounts, an entity should institute policies and procedures for authorizing logical access to information resources and document such authorizations. Resource owners should have identified authorized users and the access they are authorized to have.	These findings were for access to numerous types of applications, including financial, payroll/human resource, student, and others. They were also related to access requests for the operating systems, databases, networks, and other information technology resources. ▪ Documentation of access	21	8	9	17

EXHIBIT B (Continued)

SUMMARY OF IT AUDIT FINDINGS
BY CONTROL CATEGORY AND TECHNIQUE

Control Category	Control Technique	Description	Finding Results and Issues	No. of Findings	No. of State Agencies	No. of Educational Entities	Total No. of Entities
		Approved authorizations should be maintained on file.	authorization requests could not be provided because the documentation was not required or was not retained. ▪ Documentation of access authorization requests did not provide adequate evidence that the level of access granted was the same as requested, including not having adequate descriptions of what was being requested. ▪ Access privileges granted did not correspond to the access privileges authorized on the authorization forms. ▪ Documentation was not sufficient to determine the user's identity. ▪ Supervisory approvals were not required before access privileges were granted. ▪ There were no written procedures regarding authorization of access privileges.				
Access Controls	11. Appropriate Access Privileges	Access should be limited to individuals with a valid business purpose (least privilege).	▪ Users had application update access that was not required for their duties or allowed them to perform incompatible duties. ▪ Security administration capabilities were inappropriately granted to individuals other than security administrators. ▪ An excessive number of application users were granted correction mode access. ▪ Users had full administrator rights on their workstations. ▪ Security was incorrectly set up and allowed users more access than needed. ▪ Individuals (users and IT staff) had access capabilities in various IT areas that were not required for their duties. ▪ IT staff performed incompatible IT-related duties (sometimes with the superuser account). ▪ More people than necessary had domain administration access capabilities to administer the servers. ▪ IT staff had end-user update access to the application. ▪ Help desk staff could enter data into the application for users. ▪ Individuals had unnecessary access capability to make changes to the application data files outside application controls. ▪ Default accounts were not appropriately restricted. ▪ There were incompatible duties between system administration and security administration. ▪ Logging in using the root ID was not disabled on the production servers. ▪ There were unnecessary duplicate accounts. ▪ Users' access could not be limited to	52	14	31	45

EXHIBIT B (Continued)

SUMMARY OF IT AUDIT FINDINGS
BY CONTROL CATEGORY AND TECHNIQUE

Control Category	Control Technique	Description	Finding Results and Issues	No. of Findings	No. of State Agencies	No. of Educational Entities	Total No. of Entities
			only the finance or payroll datasets, thereby allowing some users, who only needed access to one of the datasets, to be assigned to both. ▪ Ninety-one users, including technical staff and end users, were assigned the transaction code privileges that allowed access to programs not necessary for their job functions. ▪ Contractor staff had been granted access to the application source code and administrative privileges to the application and database server and application management server software. ▪ Certain application users had an application profile that allowed access to social security administration information not needed for their job classification. ▪ A consultant had the capability of approving requisitions.				
Access Controls	12. Review of Access Privileges	Security managers should review access authorizations and discuss any questionable authorizations with resource owners. Resource owners should periodically review access authorizations for continuing appropriateness.	▪ A review of application access privileges was not being performed on a periodic basis to ensure that access privileges remained appropriate and necessary. ▪ There was no documentation of a periodic review of user access rights. ▪ The security officer assigned user roles based on the employee's supervisor's recommendation, rather than a review of the employee's position description as required by auditee policy. ▪ There were no written requirements for data owners to conduct a periodic review of access to the data for which they were responsible.	15	8	5	13
Access Controls	13. Security Administration Monitoring and Logging Controls	All changes to security access authorizations should be automatically logged and periodically reviewed by management independent of the security function and unusual activity should be investigated.	▪ Security tables were not subject to logging and monitoring. ▪ Security events were logged but they were not periodically reviewed. ▪ The application (and sometimes the database) did not have the functionality to maintain an audit log of security accesses. ▪ The system did not provide adequate logging of access privilege changes. ▪ The auditee had not implemented periodic reviews of the appropriateness of the security system settings. ▪ The history file that contained changes to file permissions, changes to file ownerships, and deletions of files had been inadvertently deleted. ▪ Logs of network access modifications made by security administrators did not exist. ▪ The security software did not have a logging function available which prevented management from reviewing access modifications made within the security software. ▪ The division did not monitor security	19	6	12	18

EXHIBIT B (Continued)

SUMMARY OF IT AUDIT FINDINGS
BY CONTROL CATEGORY AND TECHNIQUE

Control Category	Control Technique	Description	Finding Results and Issues	No. of Findings	No. of State Agencies	No. of Educational Entities	Total No. of Entities
			changes for the application or network. ▪ The division did not have security change logs for the application.				
Access Controls	14. Removal or Adjustment of Former or Reassigned Employee or Contractor Access	Inactive accounts and accounts for terminated or reassigned employees and contractors should be disabled, removed, or adjusted in a timely manner.	▪ Former or reassigned employees (or contractors) continued to have active e-mail, mainframe, operating system, network, or database accounts. ▪ A former employee's user ID was being used by programming staff to run batch programs. ▪ Users who had been given temporary update access privileges retained access privileges beyond the time frame necessary. ▪ Former employees had their user IDs used beyond their termination date and the auditee was unable to determine what activities were performed. ▪ The auditee did not document the date the employees' access privileges were removed from the application. ▪ There was no formal or timely process for notifying security administrators of employees leaving employment or changing positions. ▪ Auditee policy allowed for employees to access the auditee's network and e-mail for up to 30 days after terminating employment. ▪ Terminated employees continued to be defined as active in the network after termination. ▪ A contractor continued to have access to the source code library after his access termination request date. ▪ User accounts of former employees were not revoked timely and continued to have access beyond their termination dates.	48	13	28	41
Access Controls	15. Restriction of Access to Sensitive Data	Access to sensitive/privileged accounts should be restricted to individuals or processes having a legitimate need for the purposes of accomplishing a valid business purpose. Password/authentication services and directories should be appropriately controlled and encrypted when appropriate.	▪ The auditee collected and used certain employee social security numbers (SSNs) in the application with no specific authorization in law (in some cases as unique identifiers). ▪ The auditee did not have a policy or procedure for classification of application data as confidential, sensitive, or public; to address requests for employee-related nonpublic information; or to address physical security of documents containing nonpublic information. ▪ Auditee was inappropriately disclosing SSNs, contrary to State law. ▪ Instances were noted where vendor files containing SSNs were not adequately secured. ▪ Procedures for monitoring procurement record attachments for confidential information needed improvement. ▪ All passwords were stored in clear text.	22	16	4	20

EXHIBIT B (Continued)

SUMMARY OF IT AUDIT FINDINGS
BY CONTROL CATEGORY AND TECHNIQUE

Control Category	Control Technique	Description	Finding Results and Issues	No. of Findings	No. of State Agencies	No. of Educational Entities	Total No. of Entities
			▪ Security administrators could print a list of users and their respective passwords. ▪ User IDs and passwords were distributed in unencrypted e-mail. ▪ Steps had not been taken to ensure that staff were aware of policies regarding nonpublic information safeguards. ▪ Purchasing agreements and contracts did not contain clear and comprehensive security clauses prohibiting the disclosure of nonpublic information by vendors. ▪ There were no procedures to address cleansing or destroying electronic media that was to be disposed and some were not completely erased. ▪ Accurate documentation regarding surplus computers was not always maintained. ▪ Effective security controls had not been established for compact discs containing protected data that were distributed to other entities. ▪ The District did not adequately sanitize the hard drives of surplus equipment.				
Access Controls	16. Transmission Controls	Cryptographic tools should be implemented to protect the integrity and confidentiality of sensitive and critical data and software programs where appropriate. Encryption procedures should be implemented in data communications where appropriate based on risk.	▪ Confidential and sensitive information was not adequately protected during transmission to outside entities. ▪ Secure transmission was not used when remotely accessing the network and remote access did not go through a firewall. ▪ The auditee utilized unencrypted telnet and unencrypted file transfer protocol. ▪ Office applications were not encrypted and traffic over the network including transfer of bank accounts and SSNs was not encrypted between the District and Headquarter offices.	3	2	1	3
Access Controls	17. Monitoring and Logging Controls	An effective intrusion detection system should be implemented, including appropriate placement of intrusion-detection sensors and incident thresholds. An effective process should be established based on a risk assessment to identify auditable events that will be logged. All auditable events, including modifications of sensitive or critical system resources, should be logged. Audit records should contain appropriate information for effective review including sufficient information to establish what events occurred, when the events occurred, the source of the events, and the outcome of the events. Audit records should also be retained long enough to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	▪ The auditee had not established appropriate security standards for logging user activity within the application. ▪ The auditee lacked the capability to log user activity on the network. ▪ Logging was not enabled on the database. ▪ Although the auditee logged modifications of sensitive or critical tables, files, and transactions, there was no periodic review of the logs. ▪ The tracking list was not always reviewed daily as required. ▪ There were no logs documenting the computers for which the hard drives were erased or when and by whom the erasure had been performed. ▪ The lack of auditee monitoring and logging reports prevented the auditee from determining if generic user IDs had been used. ▪ Application, database, and network	40	11	17	28

EXHIBIT B (Continued)

SUMMARY OF IT AUDIT FINDINGS
BY CONTROL CATEGORY AND TECHNIQUE

Control Category	Control Technique	Description	Finding Results and Issues	No. of Findings	No. of State Agencies	No. of Educational Entities	Total No. of Entities
			activity and performance were not monitored. ▪ The console log did not provide sufficient detail to clearly describe the change made or identify the person who made the change. ▪ Auditee monitoring procedures did not include monitoring a subrecipient-established application's security policies and controls during the fiscal year. ▪ The auditee was unable to provide documentation showing where employees acknowledged that they had reviewed the system logs for inappropriate activity. ▪ There was no intrusion detection system installed on the production servers and the servers and network traffic were not monitored. ▪ There was no notification to IT support staff of repeated unsuccessful access attempts. ▪ The auditee did not monitor or review application security events such as accesses to and modifications of critical tables and files. ▪ Accounts with sensitive privileges did not have the audit flag enabled and the logs that were created were missing certain days' activity. ▪ Oracle database auditing was not enabled and actions taken by the system account were not recorded. ▪ There were no procedures in place regarding monitoring of security events or breaches to the applications or databases. ▪ The Department did not have available logging activated to record the activities of individuals using inherently risky application functions. ▪ Logs identifying invalid access attempts and intruder lockouts for the network were not periodically reviewed.				
Access Controls	18. Physical Security Controls	Physical security controls should be implemented to restrict physical access to computer resources including: ▪ primary computer facilities ▪ cooling system facilities ▪ network devices such as routers and firewalls ▪ terminals used to access a computer ▪ access to network connectivity ▪ computer file storage areas ▪ telecommunications equipment and transmission lines. Access should be limited to those individuals who routinely need access through the use of guards, identification badges, or entry devices such as key cards. Management should conduct a regular review of individuals with	▪ Physical access to the computer data center was not always effectively restricted. ▪ Access to the data center was not removed for individuals who had terminated employment. ▪ Sensitive, nonpublic, or proprietary information was stored in an unlocked location. ▪ Documentation did not always support adherence to the policy requirement of at least two employees being present in the vault at all times while it is open. ▪ Access to the server or network room was not restricted to only staff who required access to perform server or network maintenance work. ▪ The Department did not periodically	7	6	0	6

EXHIBIT B (Continued)

SUMMARY OF IT AUDIT FINDINGS
BY CONTROL CATEGORY AND TECHNIQUE

Control Category	Control Technique	Description	Finding Results and Issues	No. of Findings	No. of State Agencies	No. of Educational Entities	Total No. of Entities
		physical access to sensitive facilities to ensure such access is appropriate.	review the appropriateness of physical access privileges to the servers. ▪ Sixteen key fob or key pad combination assignments were not appropriate. ▪ There was a hole in the door above the door knob that was large enough to allow a person to open the door from the inside. ▪ Maintenance staff had keys providing unrestricted access to the server room.				
3. Configuration Management	1. Software Patch Management	An effective patch management process should be documented and implemented, including: ▪ identification of systems affected by recently announced software vulnerabilities ▪ prioritization of patches based on system configuration and risk ▪ appropriate installation of patches on a timely basis, including testing for effectiveness and potential side effects on the entity's systems ▪ verification that patches, service packs, and emergency fixes were appropriately installed on affected systems.	▪ Systems used versions of software that were no longer supported by the vendor. ▪ The auditee's patch management software was not a current version. ▪ The anti-virus software that was used on some desktop clients and servers did not have the current patch version installed. ▪ The operating system did not have the current patch version installed. ▪ The auditee did not require programmers to complete a record of work, including workflow authorization signatures, when implementing patches and updates for system software. ▪ Department policy had not been updated to address security patches for the Division's new operating system environment.	5	4	1	5
4. Separation of Duties	1. Database Controls	Data administration involves planning for and administering the data used throughout the entity. Documented job descriptions should accurately reflect assigned duties and responsibilities and segregation of duty principles. All employees should fully understand their duties and responsibilities and should carry out those responsibilities in accordance with their job descriptions.	▪ Policies and procedures had not been provided for database administration responsibilities and activities, and data storage procedures had not been defined.	3	0	3	3
Separation of Duties	2. Computer Operations Controls	Detailed, written instructions should exist and be followed for the performance of work. Instruction manuals should provide guidance on system operation. Application run manuals should provide instruction on operating specific applications.	▪ There were no procedures in place to ensure that all jobs were authorized and scheduled. ▪ Auditee staff did not follow established job scheduling procedures resulting in discrepancies in balances on the general ledger master file.	2	2	0	2
5. Contingency Planning	1. Environmental Controls	Fire detection and suppression devices should be installed and working (smoke detectors, fire extinguishers, and sprinkler systems). Controls should be implemented to mitigate other disasters (floods, earthquakes, terrorism). Building plumbing lines should not endanger the computer facility. A UPS or backup generator should be provided. Humidity, temperature, and voltage should be controlled.	▪ A fire suppression system was not installed at the data center. ▪ The data center had a wet pipe fire suppression system with water pipes directly over IT equipment. ▪ The division server room did not have raised floors or water detectors. ▪ The temperature and humidity in the server room were not monitored. ▪ There was no automatic monitoring of the air conditioning and it was not on a separate circuit.	4	1	3	4

EXHIBIT B (Continued)

SUMMARY OF IT AUDIT FINDINGS
BY CONTROL CATEGORY AND TECHNIQUE

Control Category	Control Technique	Description	Finding Results and Issues	No. of Findings	No. of State Agencies	No. of Educational Entities	Total No. of Entities
			▪ The fire extinguishers had a last recorded maintenance date of May 2005 and December 2000.				
Contingency Planning	2. Performance Management	Records should be maintained on the actual performance in meeting service schedules. Problems and delays encountered, the reason, and the elapsed time for resolution should be recorded and analyzed to identify recurring patterns or trends. Senior management should periodically review and compare the service performance achieved with the goals and surveys of user departments to see if their needs are being met.	▪ The auditee did not log, monitor, or review performance of the application. ▪ The auditee did not log, monitor, or review performance of the database. ▪ The auditee did not log, monitor, or review performance of the network.	2	0	2	2
Contingency Planning	3. Contingency Plan Development, Modification, and Testing	A contingency plan should be documented that: ▪ is based on clearly defined contingency planning policy ▪ reflects current conditions, including system interdependencies ▪ has been approved by key affected groups, including senior management, information security and data center management, and program managers ▪ clearly assigns responsibility for recovery ▪ includes detailed instructions for restoring operations ▪ identifies the alternate processing facility and the backup storage facility ▪ includes procedures to follow when the data/service center is unable to receive or transmit data ▪ identifies critical data files ▪ is detailed enough to be understood by all entity managers ▪ includes computer and telecommunications hardware compatible with the entity's needs ▪ includes necessary contact numbers ▪ includes appropriate system-recovery instructions ▪ has been distributed to all appropriate personnel ▪ has been coordinated with related plans and activities. The contingency plan should also be periodically tested under conditions that simulate a disaster.	▪ The auditee's security over backup tapes being transported off-site was deficient, or the off-site facility was too close to the data center. ▪ The disaster recovery plan did not address key elements such as prioritization of critical operations and data, provisions for backup personnel, allowable outage times before activating the alternate site, procedures to follow when the regional data center is inoperable, what responsibilities were assigned to the Recovery Team, and what supplies, forms, and support equipment would be needed at the alternate site. ▪ The alternate site was within close proximity to the data center and a second alternate site was not addressed. ▪ The disaster recovery plan had not been tested, or all critical applications had not been tested. ▪ The IT disaster recovery plan was in draft form and had not been officially adopted, or had not been fully implemented. ▪ Sole responsibility for disaster recovery was the responsibility of one individual without a named alternate. ▪ The disaster recovery plan had not been updated to include current software, hardware, processes, and procedures. ▪ The disaster recovery plan was not a comprehensive, management-approved document prepared based on the identification of disaster or disruption scenarios, criteria to initiate the recovery process, and recovery strategies. ▪ The auditee's signed agreement with the regional data center did not include the regional data center's commitment to resume services within two weeks of disruption of service or other responsibilities. ▪ Backup images were copied to tape only once a week and cycled off-site, hampering the Department's ability to	20	6	14	20

EXHIBIT B (Continued)

SUMMARY OF IT AUDIT FINDINGS
BY CONTROL CATEGORY AND TECHNIQUE

Control Category	Control Technique	Description	Finding Results and Issues	No. of Findings	No. of State Agencies	No. of Educational Entities	Total No. of Entities
			completely recover lost data by using the off-site backup tapes. ▪ The disaster recovery plan had not been updated to reflect current staff or current backup operating procedures. ▪ The Department did not have a Departmentwide disaster recovery plan that included procedures for annual testing and applied to all critical Department IT resources.				
6. Application Level General Controls	1. Application Program Change Controls	Entities need to proactively manage changes to system environments, application functionality, and business processes to reasonably assure financial data and process integrity. Entities should restrict and monitor access to program modifications and changes to configurable objects in the production environment. Most application configuration changes are managed using a staging process. The staging process allows the entity to develop and unit test changes to an application within the development environment, transport the changes into a quality assurance environment for further system and user acceptance testing and, when the tests have been completed and the changes are approved, transport the changes into the production environment.	▪ Programming staff did not follow established policies and procedures. ▪ No mechanism to detect and log program changes being moved to production. ▪ Program change requests lacked documentation to substantiate that the changes made were appropriately authorized, tested, and approved for implementation. ▪ Programs were programmed, tested, and moved by the same person. ▪ Programmers had access to production code and the production job scheduler. ▪ Users had update access to production code. ▪ The work order status was not closed for completed change requests. ▪ There was no supervisory review to ensure required approvals were in place. ▪ Change control standards and manuals were outdated. ▪ A user acceptance test environment did not exist. ▪ Documentation of independent testing could not be provided. ▪ Procedures did not require that program changes moved to production be logged, reviewed, or monitored by supervisory staff. ▪ The development software did not provide the capability to retain historical logs of program changes. ▪ The auditee had not activated the design lock feature to preclude concurrent development of the same program. ▪ Development software did not control developer's access to data. ▪ Change management procedure lacked provision for approvals of emergency changes and minimal ad hoc changes. ▪ Testing program changes was performed in the production environment. ▪ There was no Information System Development Methodology. ▪ The auditee did not require programmers to complete a record of work, including work flow authorization signatures, when implementing configuration changes or database upgrades.	45	14	14	28

EXHIBIT B (Continued)

SUMMARY OF IT AUDIT FINDINGS
BY CONTROL CATEGORY AND TECHNIQUE

Control Category	Control Technique	Description	Finding Results and Issues	No. of Findings	No. of State Agencies	No. of Educational Entities	Total No. of Entities
			▪ The software development plan did not document the roles of some project staff and had not been updated to reflect changes in project staff that had occurred.				
Application Level General Controls	2. Documentation Controls	Documentation should be updated when a new or modified system is implemented.	▪ Flow and management of data have not been documented for certain system functions, including financial, payroll/personnel, and student applications. ▪ The Division had not developed application user documentation. ▪ There were no user manuals, diagrams, or system documentation for the application.	3	1	1	2
7. Business Process Controls	1. Input Controls	Appropriate edits should be used to reasonably assure that data are valid and recorded in the proper format. Procedures should also be established to reasonably assure that all inputs into the application have been accepted for processing and accounted for; and any missing or unaccounted for source documents or input files have been identified and investigated. The procedures should specifically require the exceptions be resolved within a specified time period.	▪ Auditee scanning and indexing guidelines did not include provisions for supervisory or independent review of information scanned and stored in the application. ▪ The scanner used to input documents into the application automatically assigned document numbers thus providing a total count of documents scanned, but staff did not perform record counts prior to scanning and were unable to compare the quantity of documents processed to the system count. ▪ The auditee did not require adequate authentication of the data submitted on a payment form for vendors which resulted in a fraud perpetuated by a third party. ▪ There was no standardization for addresses in the application database. ▪ When group services were provided, the services for the customers within the groups were not being entered into the application.	5	4	0	4
Business Process Controls	2. Transaction Data Processing Controls	Application processing of input data should be automated and standardized. System entries should use transaction logs to reasonably assure that all transactions are properly processed and to identify the transactions that were not completely processed. Transactions with errors should be rejected or suspended from processing until the error is corrected.	▪ The auditee did not timely address processing errors resulting from the daily data upload process. ▪ There was not an automatic address cross-match between entities to determine if any sexual predator or offender addresses were in the application database. ▪ The auditee did not fully utilize all the functional capabilities available in the system and continued to rely on workarounds and alternate systems in lieu of system functionality. ▪ The salary refund calculation of net pay contained a programming error. ▪ Deficiencies continued to exist in the 2008 tax rate calculation process. ▪ A programming error existed within the approval process for compromise waivers.	6	5	0	5

EXHIBIT B (Continued)

SUMMARY OF IT AUDIT FINDINGS
BY CONTROL CATEGORY AND TECHNIQUE

Control Category	Control Technique	Description	Finding Results and Issues	No. of Findings	No. of State Agencies	No. of Educational Entities	Total No. of Entities
Business Process Controls	3. User Controls	Periodic reconciliations should be performed and exceptions should be appropriately handled.	▪ There were no procedures requiring monthly reconciliations between the audited system and FLAIR. ▪ The audited system's consolidated data was not analyzed for potential overpayments. ▪ There was no formal review by management to ensure that changes or overrides to certain application controls had been made in accordance with established State law. ▪ The auditee lacked reconciliation procedures. ▪ The auditee did not consistently document the release of output data tapes to other entities. ▪ Claims were not reviewed in a timely manner. ▪ Reports included misstatements or incorrect calculations. ▪ Exception reports were not reviewed by the appropriate administrative staff. ▪ There was no control in place to prevent a failed input file from being deleted before the file was reloaded by the assigned staff. ▪ Effective procedures for the review of the corrections of errors on the failed file did not exist to ensure that the errors were followed up on.	13	8	1	9
8. Interface Controls	1. Data Exchange Controls	Procedures should include a complete list of interfaces to be run, the timing of the interface processing, how it is processed and how it is reconciled. A positive acknowledgement scheme should be used to ensure that files sent from a source system are received by the target system. The files generated by an application interface should be properly secured from unauthorized access and/or modifications.	▪ Although data exchange errors were generated, they were deleted after seven days if not addressed. ▪ The auditee did not retain documentation evidencing that data had been requested at least quarterly. ▪ The auditee had not negotiated an agreement with another entity for the provision of data at needed intervals.	2	2	0	2
9. Data Management System Controls	1. Transaction History Logging	Logging and monitoring controls should be in place at the data management system level that effectively satisfies requirements to accurately identify historical system activity and data access.	▪ Transaction logging was either not in place within several applications or data logs only recorded the most recent user ID, date updated, and panel updated, but did not record the actual data fields changed. ▪ Although changes to data files were recorded, the information was not reviewed. ▪ Updates to datasets were not logged by the system to establish responsibility for such changes and to allow for proper monitoring and review.	3	2	1	3
		TOTAL FINDINGS		**613**			