Georgia Department of Audits and Accounts
Performance Audit Operations
Russell Hinton, State Auditor
Leslie McGuire, Director

Georgia Department of Education

Internal Control Review of the Quality Basic Education (QBE) Funding Formula

Improvements Are Needed To Strengthen Existing Controls

Why we did this review

This audit was conducted to assess the effectiveness of internal controls over the allotment of state funds to local school systems through the "Base Earnings" calculation within the Quality Basic Education (QBE) funding formula. Since many of the control activities related to QBE are incorporated in automated systems, our Department's information systems auditors assisted with this performance audit.

Who we are

The Performance Audit Operations Division was established in 1971 to conduct in-depth reviews of state programs. The purpose of these reviews is to determine if programs are meeting their goals and objectives; provide measurements of program results and effectiveness; identify other means of meeting goals; evaluate the efficiency of resource allocation; and assess compliance with laws and regulations.

Website: www.audits.ga.gov
Phone: 404-657-5220
Fax: 404-656-7535

What we found

While GaDOE has established various controls related to the state's public K-12 education funding formula, no single office or individual within GaDOE is specifically responsible for ensuring that the process for determining funding allotments is working appropriately and accurately through a purposefully designed system of internal controls. The Quality Basic Education (QBE) Act of 1985 established the state's method for providing funding to local school systems through a series of calculations called the "QBE Funding Formula." For practical purposes, the QBE funding formula is used to allocate funds among the state's 184 local school systems since the total amount of QBE funding is subject to funds appropriated by the General Assembly. In fiscal year 2008, $6.6 billion of the $15.6 billion spent on public K-12 education in Georgia was funded through this formula. Given the significant amount of state resources expended for Georgia's K-12 education each year, our review was designed to assess the effectiveness of internal controls over the process that determines QBE funding allotments, specifically the "base earnings" calculation within the QBE funding formula, which computes a foundation level of funding for each system's state-funded instructional programs.

Based on the internal control framework established by the Committee for Sponsoring Organization of the Treadway Commission (COSO) (www.coso.org), we have determined that improvements are needed in each of the five major control areas, with the most significant improvements needed in designing

controls to prevent unauthorized access and manipulation of data used in the QBE funding calculation. As defined by COSO, *internal control* is a "process…designed to provide reasonable assurance regarding the achievement of objectives in the effectiveness and efficiency of operations," the reliability of financial reporting, and compliance with applicable laws and regulations. Internal control consists of five interrelated components. A discussion of these control areas and GaDOE's efforts in each area is summarized below. It should be noted that a review of internal controls is typically the first step taken to evaluate the accuracy of reported data and the reliability of systems using such data. Weaknesses in internal controls do not necessarily mean that there are significant problems with the data or systems. However, if controls are adequate, more confidence can be placed on the results of additional testing performed to evaluate the accuracy of the data and systems.

Control Environment – While GaDOE has instituted controls related to its control environment, the control environment needs to be strengthened by setting clear ethical guidelines related to the FTE and QBE process, better evaluating the competence of local school system staff involved with the process, and forming a group to manage the process. According to COSO, the control environment sets the tone for the organization and is the foundation for all other components of internal control.

Risk Assessment – GaDOE had implemented control activities to mitigate many of the risks related to the QBE funding process; however, we found that a formal risk assessment of the process has not been performed to ensure that all significant risks associated with the proper execution of the QBE formula have been identified and addressed. According to COSO, a formal risk assessment serves as the starting point for creating a system of internal control by identifying risks, estimating their significance, assessing the likelihood of the risk occurring, and determining the actions that will help avoid the risk.

Control Activities / Information and Communication – Control activities are actions implemented by an organization to mitigate identified risks and achieve established objectives. Most of the GaDOE's QBE-related control activities and communications are incorporated in its automated information systems. For example, GaDOE's has more than 200 edit checks related to the processing of FTE data. Collectively, these edits are intended to serve as both preventive controls (to disallow incomplete or missing data records from being accepted by GaDOE) and detective controls (to identify potential data abnormalities for review and resubmission by reporting school systems). Furthermore, we found that the QBE application has numerous "business rule" calculations that use various data inputs, such as FTE counts and legislative funding decisions, to perform prescribed calculations to yield QBE allotments. Our Department's information systems auditors attempted to evaluate the effectiveness of these control activities; however, they found that weaknesses in GaDOE's IT General Controls and security vulnerabilities in its FTE and QBE systems need be addressed before an adequate assessment of underlying control activities can be conducted.

Monitoring – Our review identified several weaknesses in GaDOE's monitoring of the QBE funding process. We found that GaDOE needs to better monitor the FTE data reported by local school systems. Specifically, GaDOE needs to perform statistical analyses of submitted data to identify significant anomalies that could be investigated to evaluate the validity and accuracy of reported data and also needs to address weaknesses in its FTE Comparison Report. School systems with alternative or "block" schedules need to be better monitored to ensure that they were properly converting to standard FTE segments. In addition, we found that GaDOE did not have adequate resources assigned to monitor the control activities related to its FTE data collection process. Finally, we found that while state law requires that the Governor appoint a task force to be convened every three years to monitor and review instructional programs cost components used in the QBE formula, these components have not been reviewed in more than 19 years.

The Department of Education's written response to this report indicated that it agreed with the findings in the report and noted specific implemented (or planned) corrective actions. The actions specifically noted by GaDOE are included in the remainder of this report.

Table of Contents

Audit Purpose 1

Background 1

Findings and Recommendations 9

- Control Environment 9
- Risk Assessment 11
- Control Activities – Information Systems Controls 12
- Control Monitoring 14

Appendices

- Appendix A: Objectives, Scope, and Methodology 20
- Appendix B: Information on the 19 QBE Instructional Programs 22
- Appendix C: Cost Categories for the High School Base Program 23
- Appendix D: Information Systems Controls Review 24

Audit Purpose

The purpose of this audit was to assess the effectiveness of internal controls over information systems and business processes related to the "base earnings" calculation within the Quality Basic Education (QBE) funding formula. Our evaluation criteria was based on the internal control framework known as COSO (Committee of Sponsoring Organizations of the Treadway Commission) which is generally accepted as providing a basis for establishing internal control systems and for evaluating their effectiveness. More information about the COSCO framework is provided on page 8, and details about our objectives, scope, and methodology are included in **Appendix A.**

COSO defines internal control as a "process … designed to provide reasonable assurance regarding the achievement of objectives".

This report has been discussed with appropriate personnel representing GaDOE. A draft copy was provided for their review and they were invited to provide a written response, including any areas in which they plan to take corrective action. Pertinent responses have been included in this report as appropriate.

Background

Funding for public K-12 education in Georgia primarily comes from state and local funding sources, but also includes additional federal funding. As shown in **Exhibit 1**, the state's education funding totaled approximately $15.7 billion in fiscal year 2008

Exhibit 1
K-12 Public Education Fund Sources
Fiscal Year 2008

Fund Source	State Funding		% of State Funding	Total Funding	% of Total Funding
State Funding					
QBE Program[1]	$8,125,815,243				
Less: Local Five Mill Share[2]	(1,542,897,518)				
QBE State Funds[3]		$6,582,917,725	82.65%		
Pupil Transportation		168,868,763	2.12%		
State Interagency Transfers		318,570,915	4.00%		
QBE Equalization		485,779,211	6.10%		
All Other Programs		408,858,169	5.13%		
Total State Funding			100.00%	**$7,964,994,783**	**50.79%**
Local Funding[4]				**6,157,972,027**	**39.27%**
Federal Funding				**1,548,324,426**	**9.87%**
Other Funding				**11,728,436**	**.07%**
Total Funding				**$15,683,019,672**	**100.00%**

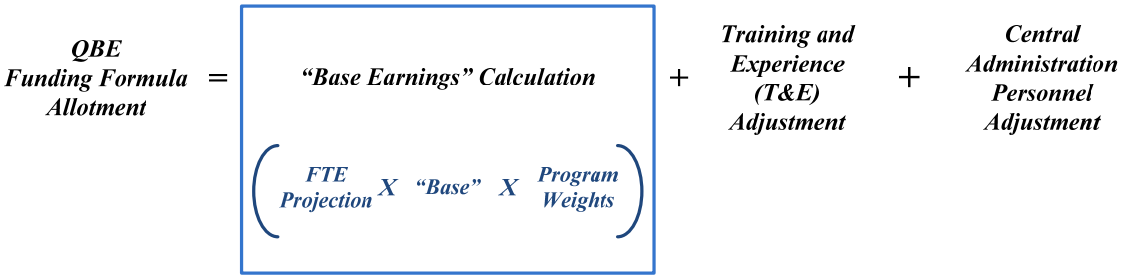
[1] The overall QBE Funding Formula determines this total; however, it may be adjusted by austerity reductions and the Georgia Special Needs Scholarships (GSNS).
[2] The Local Five Mill Share (LFMS) represents five mills of property taxes in each school district (local tax revenues) although they are included in the total QBE Funding Formula.
[3] The resulting state portion of the total QBE allotment.
[4] GaDOE's estimate of locally generated funds expensed on K-12 education.

Source: SAO Budgetary Compliance Report

(the most recent audited information available at the time of our review). The Georgia Department of Education (GaDOE) expended just under $8 billion of state funds in fiscal year 2008, of which approximately $6.6 billion (42% of all funds, 83% of state funds) was through the QBE (Quality Basic Education) Program budget, as derived through what is called the "QBE Funding Formula."

QBE Funding Formula

The Quality Basic Education (QBE) Act of 1985 established a method for calculating the state's financial contribution to public education via a series of calculations called the "QBE funding formula." When executed, the QBE funding formula generates funding allotments provided to local school systems, the total of which was approximately $8.1 billion in fiscal year 2008 (see **Exhibit 1** on the previous page). The school systems in turn determine the amount allocated to their individual schools. The QBE funding formula can be summarized as:



The "base earnings" calculation, which is the primary focus of this report and is discussed in more detail in following sections, calculates a foundation level of funding. Onto this foundation, a separate Training & Experience (T&E) calculation adds state funding to provide adjustments for the relative salaries of teachers and other personnel, such as school administrators (based on the certification and experience levels they have attained[1]). Furthermore, salaries for central administrative staff positions, such as superintendents, assistant superintendents, and accountants, are also added to each school system's QBE allotments through the Central Administration Personnel Adjustment. These three pieces added together result in the Total QBE Funding Formula Allotment.

State law also specifies how the components in the formula are calculated. It should be noted that the QBE funding formula is used as both a planning tool during the budgeting process as well as the state's official allotment calculation to determine each school system's QBE earnings.

[1] The base earnings calculation assumes that all funded staff positions, most of whom are teachers, earn only an entry-level salary, which is defined as a bachelor's degree with no creditable years of experience. Another application called Certified Personnel Information (CPI) provides information on teacher education and teaching experience that is used in the Training and Experience calculation.

QBE Base Earnings Calculation

The base earnings calculation within the overall QBE Funding Formula computes a foundation level of QBE funding for each of a local school system's state-funded instructional programs. According to various sections in OCGA 20-6-2, these funds are intended to provide state funding towards the personnel and operational cost categories that are associated with each instructional program. There are currently 19 QBE-funded instructional programs, e.g., Grades 1 – 3 (primary grades), Grades 9 - 12 (high school), and Remedial Education. (**Appendix B** lists the QBE-funded instructional programs along with a description of each program's general purpose and other information.) **Exhibit 2** provides an example of the base earnings calculation for the primary grades program in one system.

Exhibit 2
Example QBE "Base Earnings" Calculation for a Local School System Primary Grades Program

375	*X*	*$2,642.32*	*X*	*1.2841*	=	*$1,272,376*
Full-Time Equivalent (FTE) Projection		*Base Cost*		*Program Weight (Grades 1-3)*		*Total Allocation*

In this example, a school system with 375 full-time equivalent students (FTE) in its Grades 1-3 instructional program for fiscal year 2008 will receive approximately $1.27 million in base earnings. This calculation is performed for each of the QBE-funded instructional programs that a school system operates. The base earnings calculation is the most significant part of the QBE funding formula as it accounts for approximately $5.7 billion (more than 70%) of the total $8.1 billion of state funding for fiscal year 2008.

Full-Time Equivalent (FTE)

One FTE (Full-time Equivalent student) represents six periods, or segments of state-funded instruction in a typical school day.

One of the most significant components of the QBE base earnings calculation is the measurement of instructional activity that a school system provides in a given year. For QBE funding purposes, this unit of measurement is a full-time equivalent student, or FTE. One FTE represents six periods, or segments, of state-funded instruction in a typical school day. An FTE is not the same as a "student."

Since some schools use daily schedules that are not six segments (such as a four-period "block schedule"), FTE data has to be converted into the required six-segment format. The GaDOE Office of Technology Services (OTS) provides school systems with instructions on how to perform this conversion through the "FTE Data Collection-General Information" document posted on the GaDOE website. Additional instructions are provided in this guide for converting five and seven segments schedules as well.

In order to capture FTE data to be used in the funding calculation, GaDOE requires all 184 local school systems that receive state education funds to submit FTE data twice per year, once in October and again in March[2]. The specific data elements required in each reporting period, the required data format, and error correction procedures are determined by GaDOE and communicated to school systems through the GaDOE website. This process is managed within GaDOE by its OTS, and each local school system designates an FTE Coordinator. Local school systems often hire a data processing vendor as well to assist them with this process.

For each FTE reporting period, GaDOE designates an official count day on which student attendance and class schedules are recorded. For example, on the designated count day, a high school student may spend four periods (segments) in classes counted under the Grades 9-12 program while two other segments may be spent in classes under the Gifted program (see **Appendix B** for a description of each instructional program). The school systems collect this information on all students and then submit the data electronically to OTS.

When OTS receives the data, its FTE information system application begins processing the data via pre-determined edit rules. Errors caught by these rules are reported back to the school systems, which may require correction and a resubmission of the entire data file. This iterative FTE data reporting process can take approximately three weeks.

Once the reporting period ends, the FTE application totals up the reported segments for each QBE program and divides by six to yield the FTE count (**Appendix B** shows a projected state total FTE count for fiscal year 2008 for each program). Each November, GaDOE provides the Governor's Office of Planning and Budget (OPB), the House Budget Office (HBO), and the Senate Budget and Evaluation Office (SBEO) with a spreadsheet summary of the FTE counts for all school systems. However, since student enrollments may change during the year, OCGA 20-2-160 requires that the "base earnings" calculation use a projected FTE average for that year. The FTE projection is based on the three most recent FTE counts – the most recent October FTE count, the March FTE count in the same calendar year, and the prior year's October FTE count. This FTE projection is used in the base earnings calculation.

Base Unit Cost (Base) Amount

After the FTE data is summarized into FTE counts, the Base Unit Cost, or simply the "base," is determined. The base represents the funding provided for one FTE in the Grades 9-12 program (this base cost is used in the cost calculation for all programs). The Grades 9-12 program is designated as the base instructional program as it is the least expensive of all 19 QBE-funded programs. For fiscal year 2008, the base amount was $2,642.32 for one FTE.

Sections within OCGA 20-6-2 indicate there are currently 15 different cost components that make up this total. **Appendix C** presents these cost components (or Cost Categories) and the per-FTE amounts associated with each for the Grades 9-12 Program in fiscal year 2008. Each of these components may be composed of

[2] There is also a December FTE count but this does not impact QBE funding calculations.

underlying calculations. For example, the per-FTE amount for teachers of $1,830.29 is composed of the following underlying variables (or sub-categories):

- The funding ratio of one teacher for every 23 students,
- the entry level salary (four-year degree and no experience) on the state salary schedule,
- the state contribution rate (%) to the Teachers Retirement System,
- the state contribution rate (%) to the State Health Benefit Plan,
- the state contribution rate (%) for Medicare, and
- funding for 8 days of sick leave.

During each legislative session, underlying variables and cost components of the base amount may be adjusted, thereby impacting the total per-FTE base amount. Since fiscal year 2004, the only changes made were to personnel cost components (e.g., state salary schedule, benefit categories) and to media materials. According to GaDOE personnel, the final decisions made in the appropriations process are officially communicated through the "comparative summary" (i.e., the Tracking Documents of the General Appropriations Act). The base amount is also specifically stated in the General Appropriations Act.

Changes to cost components are subsequently updated in the official QBE base earnings calculation that is executed by the QBE information system application. It should also be noted that the GaDOE Budget Office, as well as OPB and HBO[3] have their own spreadsheet models of the QBE formula which are used in the budget planning process.

Program Weights

In addition to the adjustments made to the per FTE base program amounts, adjustments to the underlying variables and cost components are also made to the other 18 instructional programs (using the same basic process described previously). After adjustments are made, a funding weight is calculated for each program by dividing the total per-FTE funding amount by the base amount. For example, for fiscal year 2008 the Grades 1-3 program weight was 1.2841, based on the Grades 1-3 per-FTE funding level of $3,392.99 divided by the $2,642.32 base amount. In other words, school systems will receive 28.41% more funding per FTE in the Grades 1-3 Program than for an FTE in the Grades 9-12 Program in the base earnings calculation. **Appendix B** shows the calculated weights for each of the 19 QBE-funded programs for fiscal year 2008.

Although many of the cost categories (e.g., teachers, staff development, operations) are the same across QBE programs (e.g., Grades 1-3, Grades 9-12, Remedial), the specific values defined for each program may differ significantly. Most notably, the designated funding ratio of teachers to students has the greatest impact on the resulting total per-FTE funding level, and therefore, the greatest impact on program weights. For example, the funding ratio of teachers to students in the Special Education Level IV program was 1 to 3 in fiscal year 2008, much higher than the

[3] The Senate Budget and Evaluation Office (SBEO) reported that it is currently in the process of developing its own spreadsheet model.

funded ratio of 1 to 23 for the Grades 9-12 base program. In addition, most of the cost categories are impacted by the salary schedule variable; specifically, 10 of the 15 cost categories identified in the base program are linked to the state salary schedule amount.

The program weights are also codified in OCGA 20-2-161; however, the actual weight used in the final QBE base earnings calculation are allowed to vary from this codified weight by as much as 1.5%. (**Appendix B** also shows the codified weight in addition to the actual weight used for fiscal year 2008.) If funding decisions in the appropriations process result in a weight that is outside the allowed 1.5% range, the weights in Georgia Code must be changed; according to HBO staff, the codified weights typically have to be changed every three or four years.

Midterm Adjustment

The three base earnings calculation components (FTE, base, and program weights) are determined either before or during the legislative session in preparation of the budget for the next fiscal year. However, during the next legislative session (which occurs in the middle of that fiscal year), the QBE base earnings calculation is updated with the more recent March and October FTE counts. Interviews conducted during the engagement also indicated that although any funding variable, such as the state salary schedule, funding ratios, and operational funding amounts, may be adjusted at this time, it is typical that only the FTE data is updated to calculate the additional funding provided through the midterm adjustment.

Information Systems Used in the QBE Process

In the determination of the FTE, base, and weight components of the QBE base earnings calculation, there are two primary information system "applications" that GaDOE has built in-house to collect and process data – the FTE application and the QBE application.

FTE Application

Student data for each school system is uploaded to the FTE application via GaDOE's web portal. Each school has its own unique location code within the portal. Once access is granted, designated school system staff members have the ability to upload the required student data using flat text files. This information is then securely uploaded via FTP (File Transfer Protocol).

Before the data transmission is processed, pre-validation checks are run to ensure that each file has been properly formatted and that no "NULL" (unknown) values exist. If the pre-validation fails, the data transfer is rejected and the school receives an error message stating that correction and resubmission is required. If pre-validation is successful, the data is run through a series of edit checks (209 checks as of July 2009) as it is imported into a database. Many of these edits check for invalid data, such as the specific data fields not being left blank by the reporting school system (i.e. no "NULL" values) or incorrect character types reported in certain fields (e.g. numeric characters in a student name field). However, other edit checks attempt to identify abnormalities in a reporting school system's data. Based on our review, many of these edit checks fall into the following categories:

- **Program code checks** compare the program code provided to other information reported about a student to assess validity. For example,

verifying that students reported with a "Georgia Virtual School Program" (PROGRAM CODE = "5") are in GRADE LEVEL "6-12 only."

- **Demographic field checks** determine if a student's age, race, gender, etc., are consistent with other information. For example, comparing a student's DATE OF BIRTH to his or her reported GRADE LEVEL.
- **Student ID-based checks** compare GaDOE-assigned identification numbers and/or social security numbers to detect data abnormalities. For example, cross-checking all of a school's active STUDENT ID numbers to detect and disallow duplicate numbers.
- **Withdrawal code checks** validate that the reported reason for a student's withdrawal from a school is appropriate given other factors. For example, a student record reported as withdrawing from one school and transferring to another public school in Georgia (WITHDRAWAL CODE = "T") must also appear in the FTE data for the transfer-in school.

If an error occurs, a warning message is generated and communicated to the appropriate school system via web interface. Depending upon the error, schools may have to resubmit the data or enter a comment to explain or justify the data. Additional error checks are performed; however, these checks are designed to flag abnormalities in data that do not necessarily prohibit processing (i.e., a numeric character in a student's name). Once all edit checks run successfully, the files are written to FTE's production database. During this process, the user accounts are appended to the FTE files to ensure that user actions are tracked and recorded.

Once the FTE student data submission window is closed, the master data file for FTE is archived within another database. The data is then kept in a "static state" and not moved again until it is transferred into the QBE database for further processing.

QBE Application

Actual funding allotments earned by each school system are officially calculated in the QBE application. The QBE Application also generates other reports which are publically posted on the GaDOE website. In order to obtain access to the QBE application within GaDOE's web portal, unique user accounts are manually added to specified tables within the QBE database. Additionally, a link to the QBE application must be added to each user's portal view in order to permit access. Users can then access QBE using their normal portal account login information.

The data sets for the FTE and QBE applications are stored on the QBE database; however, the data sets are separated using two unique schemas[4]. Different user ID's are required to access data on the separate schemas. A copy of FTE data is pulled into QBE's schema when the QBE application is run. No additional error checks take place once the data has been pulled into the QBE database. The last update to QBE is stamped to identify who made the update and stored along with the data output. The QBE base earnings calculations within the QBE application are performed using aggregated data and are separated by school and program. Additionally, the application has been designed to monitor event logs. The system reviews the logs and sends email alerts to the specified team members when certain system

[4] A schema is a collection of logical structures created by users to contain, or reference, their data; they may include structures like tables, views, and indexes.

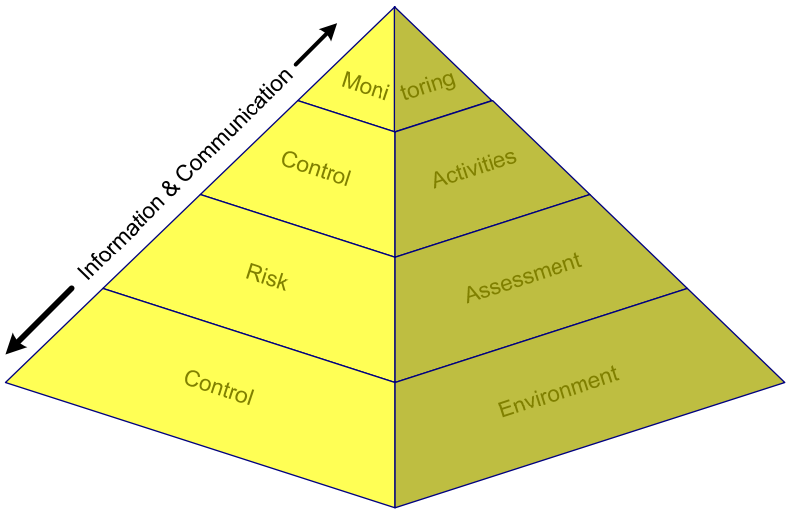
conditions occur to ensure that the data is processed by the application properly. Once the data has been processed, the output file is stored until it is ready to be published via website reporting.

Internal Control Review Framework

The internal control framework known as COSO (Committee of Sponsoring Organizations of the Treadway Commission) is generally accepted as providing a basis for establishing internal control systems and for evaluating their effectiveness. The COSO framework defines internal control as a "process…designed to provide reasonable assurance regarding the achievement of objectives" in, among other categories, the "effectiveness and efficiency of operations". The COSO framework is typically expressed as a pyramid (see **Exhibit 3**) and has five elements:

- **Control Environment**: The "tone at the top"; management's attitude towards control.
- **Risk Assessment**: The extent to which management has identified risks and established goals or objectives.
- **Control Activities**: Actions implemented to mitigate identified risks and achieve established objectives.
- **Information and Communication**: Information flow processes and how documentation is produced and distributed.
- **Monitoring**: Management's review of the control process to assess its proper functioning.

Exhibit 3
The COSO Internal Control Framework



Source: COSO (Committee of Sponsoring Organizations of the Treadway Commission)

In planning the audit, we consulted the COSO Internal Control framework and used COSO as a general guide in conducting the fieldwork under this engagement.

Findings and Recommendations

Control Environment

Under the COSO framework, the **Control Environment** is the foundation for all other internal control components. It is the tone or "corporate culture" of an organization, which reflects management's emphasis on integrity, ethics, and competence. Ethical values and policies should be set by management and clearly communicated to staff at all levels of the process. Staff should have the appropriate amount of training for their position, and the responsibilities of a position should reflect the limitations of a staff member's training and experience.

We found that GaDOE has instituted some controls related to its "QBE control environment." For example, GaDOE's staff sign a code of ethics statement annually. GaDOE conducts annual training on FTE data collection at several locations in the state that is available to local school system personnel. In addition, GaDOE staff reported that some management oversight related to the QBE process is provided by a group of upper-level financial personnel that meet as needed to discuss the GaDOE budget.

However, as discussed in the following finding, we found several areas in which GaDOE's QBE control environment needs to be strengthened.

GaDOE should strengthen its "QBE control environment" by setting clear ethical guidelines related to the FTE and QBE process, better monitoring the competence of local school system staff involved with the process, and forming a group to manage the process.

To strengthen the general control environment related to the QBE funding process, we recommend that GaDOE consider the following actions.

- **Integrity and Ethics** - GaDOE should establish specific ethical requirements or policies to clearly communicate its expectations regarding the FTE and QBE process to its staff and to personnel at local school systems. The current general ethics statements signed by GaDOE staff do not include specific ethical requirements related to the QBE process and no requirements related to the QBE process are communicated to local school system personnel. In addition to clearly identifying expected standards of ethical behavior, the policies should identify penalties for improper behavior. Once the ethical requirements and penalties are clearly identified, GaDOE should be prepared to take appropriate action when problems are identified to communicate the proper message and to strengthen its control environment.

- **Staff Competence and Job Knowledge** - GaDOE should develop mechanisms for monitoring the competence of FTE coordinators and other local school system personnel involved with the QBE process. Currently, GaDOE requires that every school system designate an FTE coordinator and makes annual training on the FTE process is made available to these coordinators and other local system personnel. However, GaDOE does not monitor the competence of FTE coordinators by tracking errors to identify

the weaknesses of individual coordinators or to identify trends or patterns of problems involving multiple coordinators. By evaluating the competence of FTE coordinators, GaDOE can better identify weaknesses so it can provide specialized training and/or take other action as necessary.

- **Management Direction and Oversight** - GaDOE should organize a group to provide its FTE and QBE process with better oversight and direction. While GaDOE staff reported providing some management oversight over the QBE process through meetings focused on budgetary needs, GaDOE does not currently have a designated person or group responsible for the activities related to implementing the QBE funding formula. Organizing a group that would be responsible for maintaining adequate FTE and QBE formula controls could help ensure that risks are properly assessed (see the finding on page 11), that control activities adequately address significant risks (see the finding on page 12) and that control activities are adequately monitored (see the findings starting on page 14).

GaDOE Response: *GaDOE reported that it concurred that strengthening the QBE control environment is needed and noted that it intended to do the following:*

- *Legal services will review the assurances signed by the local superintendents when FTE data is submitted to GaDOE to determine if the assurances contain appropriate ethical requirements and penalties for improper behavior.*
- *Technology services will have training sessions for FTE coordinators. These training sessions will begin in summer 2010 that will include such topics as: understanding the data reporting process, understanding data reporting requirements, timeliness, its purpose, who to contact, understanding business rules, and creating a calendar of events.*
- *A group will convene to conduct an end-to-end review of the QBE and FTE process.*

Risk Assessment

The COSO framework defines **Risk Assessment** as the identification, analysis and management of relevant risks to achieve established objectives. COSO specifically notes the need to identify and deal with risks associated with change.

Our review identified that GaDOE has implemented numerous information system control activities related to the QBE funding process that are intended to mitigate risks, such as data validity edit checks in the FTE application and requiring local school system superintendents to approve the FTE data before it is submitted to GaDOE. GaDOE also reported that it has performed some informal risk assessments within individual business units.

However, as discussed in the following finding, GaDOE needs to develop a formal risk assessment process to help ensure that all significant risks to the proper execution of the QBE funding process have been identified and addressed.

GaDOE needs to develop and implement a formal risk assessment process to identify and mitigate risks related to its objectives for the QBE funding formula.

While GaDOE has developed control activities to address many of the risks related to the QBE funding process, it has not implemented a formal risk assessment process to help ensure that all significant risks are addressed. A formal process helps ensure that risks are identified and addressed in a consistent and comprehensive manner and serves as the starting point for creating a strong system of internal control. An inadequate risk assessment process can result in control weaknesses. For example, our review found weaknesses with GaDOE's controls related to system access (see pages 12-13) and with its control monitoring (see pages 14-19).

GaDOE should develop a formal risk assessment plan related to its QBE funding process that includes the following components.

- A formal process to comprehensively identify risks related to QBE-related objectives. This process should also periodically reassess risks to compensate for growth, the impact of new legislation, changes in information systems and other changes in the organization's environment. In addition to risks related to an organization's objectives, the formal risk assessment should evaluate the risk of fraud related to the organization's activities.
- A prioritization system to help ensure that significant risks are adequately addressed. Since it is usually not effective, or in many cases even possible, to address all risks faced by an organization, risks must be evaluated and compared in order to prioritize mitigation efforts in order to most effectively utilize available resources.
- Strategies to develop control activities to address and mitigate significant risks and a system to monitor implementation of these strategies.

GaDOE Response: *GaDOE reported that it concurred with the finding and noted that it planned to conduct a formal risk assessment of the QBE and FTE process. The risk assessment will: identify risks (including the risk of fraud); prioritize risks; prioritize mitigation efforts; develop control activities, and develop a system to monitor the control activities. In addition to conducting the risk assessment, GaDOE will create an operations manual for staff involved with the process. The operations manual will include a flowchart and step-by-step description of the process.*

Control Activities - Information System Controls

The **Control Activities** component of the COSO framework include actions implemented by the organization to mitigate identified risks and achieve established objectives. COSO's Information and Communication component recognizes that pertinent information must be identified, captured, and communicated in a form and timeframe that enables people to carry out their responsibilities.

We determined that most of the QBE-related control activities implemented by GaDOE reside in the automated information systems managed by the Department's Office of Technology Services (OTS). Similarly, we found that much of the QBE-related information that flows within and outside GaDOE is generated by these information systems. Our review identified that GaDOE has implemented numerous information control activities that are intended to provide confidence in the reliability of FTE data and in the accuracy of the QBE base earnings calculations. Perhaps one of the most significant of GaDOE's FTE control activities is the more than 200 edit checks related to the processing of FTE data. Collectively, these edits are intended to serve as both preventive controls (to disallow incomplete or missing data records from being accepted by GaDOE) and detective controls (to identify potential data abnormalities for review and resubmission by reporting school systems). Furthermore, we found that the QBE application has numerous "business rule" calculations that use various data inputs, such as FTE counts and legislative funding decisions, to perform prescribed calculations to yield QBE allotments.

However, as summarized in the following finding, our Department's information systems auditors found information system control weaknesses related to system access and monitoring that need to be addressed before substantive tests on FTE edit checks and QBE business rules (to evaluate the adequacy or effectiveness of these controls) can be performed. They also noted that while ineffective IT controls do not preclude reliance on management's data, ineffective controls increase audit risk.

Information systems auditors identified weaknesses in the design and operating effectiveness of GaDOE's IT General Controls, including access to systems and monitoring of system changes, as well as security vulnerabilities within the GaDOE's FTE and QBE systems. These weaknesses will need to be addressed before an adequate assessment of underlying rules and edits can be conducted.

The following is a summary of the information systems control weaknesses and security issues that our information systems auditors have determined pose the highest risk to GaDOE. The detailed findings and recommendations resulting from their review are contained in a "Technical Report" that was provided to GaDOE management. Due to the sensitive nature of the information, Technical Reports are considered confidential and are only provided to those with a specific business need. A high-level overview of findings resulting from this IT internal control review are discussed below and are included in **Appendix D** starting on page 24.

- **IT Entity-Level Controls:** A review of entity-level IT controls revealed that formal IT security and change management policies and procedures are not maintained, updated, or enforced. In addition, at the time of the IT review, password policies were not in line with best practices and there was no

formal IT risk assessment framework in place.

- **IT General Controls:** IT General Controls (which include both logical access and change management controls) were assessed to determine if they provide reasonable assurance that application and IT-dependent manual controls are designed to function effectively over time and help ensure that data maintained in information systems is accurate and reliable. Information systems auditors found the following weaknesses in logical access controls: excessive and inappropriate administrator access; inappropriate identification and authentication of users; inadequate password configurations; and a lack of administrator access monitoring. In terms of IT change management controls, segregation of duty conflicts were identified. In addition, GaDOE's change management document tool was not being appropriately utilized.

- **Vulnerability Assessment:** Information systems auditors conducted a vulnerability or "attack and penetration" review to identify security exposure and business risks created by internet-facing infrastructure, threats within GaDOE's trusted network, and vulnerabilities associated with web applications that could lead to potentially unauthorized access. This review revealed insecure SQL queries that allow exposure to an attack on a database-driven website in which the attacker could execute unauthorized SQL commands. Other problems identified include: shared local administrator passwords across operating system environments; servers configured with default user name and passwords; sensitive data transmitted utilizing ineffective cryptographic controls; vulnerable software versions; sensitive information stored in clear text in database; and incidents not effectively identified and logged.

Due to weaknesses in the design and operating effectiveness of IT General Controls as well as indentified security vulnerabilities within the FTE and QBE application environments, information systems auditors determined that they could not provide reasonable assurance that application and IT-dependent manual controls continue to function effectively over time. Given these weaknesses, further procedures were not completed to determine the completeness and accuracy of QBE base earning calculations. It should be noted, however, that while ineffective IT controls do not preclude reliance on the data, they do increase audit risk. In addition to implementing the specific recommendations in the Technical Report to address these issues, our information systems auditors recommend the following activities to increase the security posture of GDOE's network and related infrastructure.

- Address all identified vulnerabilities and perform regression testing
- Develop formal server configuration and deployment procedures

GaDOE Response: *GaDOE reported that it concurred with the finding and identified specific actions (see end of* ***Appendix D****) that it is taking to correct the issues noted by our information systems auditors.*

Control Monitoring

Our audit reviewed how GaDOE oversees and manages its control process (which is referred to as "monitoring" under the COSO framework) related to its FTE and QBE applications. Monitoring is an important aspect of an effective system of internal controls as it helps provide reasonable assurance that control activities operate as intended and that they continue to operate effectively. According to COSO, some monitoring activities may be ongoing when they are built in to the internal control process and are reviewed in real time with the control activities. Additionally, organizations may conduct separate monitoring evaluations with a more broad view of the system of internal controls and its effectiveness.

Our review specifically evaluated monitoring performed by GaDOE personnel to ensure that controls were operating as intended and we identified various monitoring activities related to GaDOE's system of internal controls over QBE. For example, GaDOE, HBO, and OPB each have their own spreadsheet model of the QBE formula, including the base earnings calculation, and they independently monitor the resulting QBE allotment calculations. These groups also reported that they compare calculation results to ensure consistency. In addition, the State Government Division (SGD) of the Department of Audits and Accounts performs annual audit procedures on components of the QBE formula, such as verifying the base earnings calculation results for a sample of school systems and ensuring programs weights used in the base earnings calculation are compliant with the 1.5% allowed variance per state law. SGD staff performing these procedures reported they have had no audit findings in these areas for the past few years.

However, our review also identified weaknesses in GaDOE's monitoring of its control processes concerning FTE data and QBE calculations which are discussed in following findings.

GaDOE needs to better monitor the FTE data reported by local school systems, including making more effective use of its FTE Comparison Report, in order to more adequately evaluate the accuracy and reliability of FTE data.

Local school systems report hundreds of data elements (such as student demographic and course enrollment information) to GaDOE during the FTE data reporting process in October and March of each year. As discussed below, our review found that GaDOE needs to do more to effectively monitor the quality and accuracy of this data.

Statistical Analysis Is Not Used To Evaluate FTE Data

Currently, GaDOE does not perform any statistical analysis to identify data anomalies, or trends worthy of further investigation. An example of this type of statistical analysis might be a review to identify school systems with a disproportionate number of students in programs with the highest funding weights. We reviewed the 10 highest weighted FTE programs for the October 2007 FTE count, and identified 64 school systems that had a significantly higher proportion of their students in these high cost programs (see **Exhibit 4** below). It should be noted that this type of statistical analysis only identifies areas in need of additional research since a system's variance from the norm may be justified.

Exhibit 4
FTE Distributions in 10 Highest Weighted QBE Programs
October 2007

QBE Program	FTE Funding Weight for FY 2008	Average FTE Reported in October 2007 (% of total student population)	Number of School Systems More Than Three Times Above Average
Special Education Level IV	5.7995	0.47%	0
Special Education Level III	3.5763	2.94%	0
Special Education Level II	2.8078	0.71%	6
ESOL	2.5234	0.82%	5
Special Education Level V	2.4548	0.52%	30
Special Education Level I	2.3892	0.95%	0
Kindergarten EIP	2.0448	0.78%	7
Primary Grades EIP	1.7992	1.76%	7
Upper Grades EIP	1.7934	0.98%	8
Gifted	1.6642	3.50%	1
TOTAL			**64**

Source: GaDOE Reports

Improvements are needed in GaDOE's FTE Comparison Report

GaDOE calculates the change (both in number and percentage) in the FTEs reported for each instructional program over the previous year within each school system. Depending on the results of this calculation, these changes may appear on an FTE Comparison Report that is available for review by OTS staff. **Exhibit 5** below summarizes this report's FTE change categories and required actions. GaDOE's October 2008 FTE count identified 290 programs that had a greater than 50% change (230 had a greater than 50% increase and 60 had a greater than 50% decrease) which required explanation and review by OTS.

Exhibit 5
Changes in proportion of FTEs for School Systems

Percent Change From Prior Year	Required Reporting	Required Action
0% to 25%	None	No action required
>25% to 50%	Warning message sent to reporting school system. Not shown on FTE Comparison Report	No action required
>50%	Warning message sent to reporting school system Record of Occurrence shown on FTE Comparison Report	School system required to respond with a written explanation. OTS staff required to review explanation and approve.

Note: To avoid triggering responses for small program, the number of FTE's must change by at least 10 in addition to the percentages identified above in order to appear on the FTE Comparison Report.

Source: GaDOE FTE Comparison Report, OTS interviews

While the FTE Comparison Report provides some monitoring information on trends in FTE count data, we identified the following weaknesses with the report:

- **The percentage thresholds established in the report are relatively high**. Currently, an instructional program's FTE count has to change by more than 50% (increase or decrease and a minimum change of 10 FTEs), over the prior year before any action is required. Changes from more than 25% up to 50% only trigger a warning message being sent to the reporting school system (are not shown on the Comparison Report and no GaDOE action is required), and the report does not capture or log any changes of 25% and below. In addition, the report does not identify programs that have exhibited a pattern of increase (or decrease) slightly above or below cutoffs. (For example a program that has had 49% increases for multiple years.)

- **GaDOE does not adequately review local school system justifications for FTE changes above 50% for instructional programs.** GaDOE only requires school systems to provide a brief text response to explain FTE changes above 50% which typically does not provide sufficient information for adequate review. Of the 290 instances in which FTE changes of more than 50% (increase or decrease) in October 2008 over October 2007 were reported, 134 responses indicated that the change resulted from a "structural change", such as a new scheduling system or a change in class sizes. Fifty-eight responses simply restated that there was an increase or decrease in students for those programs and six responses indicated that the changes were due to FTE reporting errors in the previous year. GaDOE has no standard procedures regarding verification of the explanations and while there is a separate field in the FTE system for OTS staff to document what they did to confirm and approve these explanations, no notes were made in any of the cases for October 2008 and no other documentation about any reviews that might have been performed was maintained. In addition, there was no evidence of reviews by personnel in GaDOE units with more knowledge of specific instructional programs (e.g., special education) that could better evaluate reasons for significant FTE changes.

- **The FTE Comparison reporting system was not functioning for the Middle Grades and Middle Schools Programs for the two years we reviewed**. During our review, we noted there were no warnings for either of these programs while all other programs had at least one warning. Subsequently, OTS discovered the FTE comparison reporting system was not working properly for these two programs and reported that they fixed the problem and that it should function properly for the next FTE reporting cycle.

GaDOE should improve on the monitoring it performs related to controls over FTE data reported by local school systems. Statistical analyses of FTE data should be performed to identify significant anomalies that could be investigated to evaluate the validity and accuracy of reported data. In addition, GaDOE should address the weaknesses identified with the FTE Comparison Report to make this a more valuable monitoring tool. GaDOE should also ensure that staff with appropriate knowledge and experience (e.g., staff from programs such as the Gifted and Special Education Programs) are involved with these monitoring efforts.

GaDOE Response: *GaDOE reported that it concurred with the finding; however, it noted that it felt that additional staffing was needed to conduct the in-depth analysis mentioned in the report. It also noted that the FTE Comparison Report along with other FTE reports are designed to identify anomalies and that its Technology Services will review the percentage thresholds set in the FTE Comparison Report for reasonableness.*

School systems with alternative or "block" schedules need to be better monitored to ensure that they are properly converting to standard FTE segments.

GaDOE provides school systems with instructions on how to convert four, five, and seven-segment schedules into six "standard" segments before submitting FTE data. According to GaDOE, at least 235 schools received a waiver to use alternative schedules during fiscal year 2009. Our review found that GaDOE does not verify whether FTE data from these alternative schedule schools is correctly converted and reported. OTS staff reported that since FTE data has already been converted into six segments there is no way to verify that school systems are following the conversion instructions. They also reported that they do not request or receive any supplemental information that could be used to verify the accuracy of conversions performed by the school systems.

Improper segment conversions could result in funding errors. For example, a four-segment "block schedule" school should report two of its six segments from the day prior to the official FTE count day; specifically, the highest and lowest weighted programs of the four segments on the prior day. However, if two highest weighted segments are reported, GaDOE would not be able to identify this error and the school system might receive unjustified funding.

GaDOE should design monitoring procedures to verify that school systems are correctly converting block schedules to standard FTE segments. GaDOE could redesign the FTE application to require additional data from systems that do not use the standard six-segment schedule that could be used to verify the accuracy of conversions performed by the school systems. Alternatively, GaDOE personnel could make site visits to a sample of school systems to audit their conversion calculations.

GaDOE Response: *GaDOE reported that it agreed with the audit's assessment that school systems with block schedules need to be better monitored. It also noted that presently it gives detailed instructions to school systems with schedules not based on six segments on how to convert their schedules to six segments, but thought that to truly test if school systems were converting their schedules correctly would require site visits to verify source documentation. Finally, GaDOE reported that it does not have the staff to perform these site visits at this time.*

GaDOE does not have adequate resources assigned to monitor the control activities related to its FTE data collection process.

While GaDOE has various control activities integrated into its FTE reporting systems, our interviews with GaDOE staff indicated that there are no personnel that are specifically responsible for reviewing, analyzing or verifying the accuracy of FTE data being reported by local school systems for QBE funding purposes in a comprehensive way. For example, as discussed in the finding starting on page 14, GaDOE has FTE Comparison Reports that provide information on trends in FTE count data; however, no one is responsible for researching questionable trends identified by these reports. GaDOE personnel reported that they check to ensure that school systems have provided some explanation on questionable trends and may forward information on these trends to GaDOE personnel involved with individual programs; however, there is no reporting on any research that may be conducted to evaluate the questionable trends or the underlying validity of the FTE Data. In addition, GaDOE reported that there are no personnel available to conduct additional data verification evaluations like the statistical analysis techniques recommended on page 16 of this report.

GaDOE reported that it had personnel responsible for auditing and evaluating FTE data until the previous State Superintendent of Schools eliminated the last of these positions in fiscal year 1992. Furthermore, although GaDOE staff thought that the Governor's Office of Student Achievement (OSA) might perform such reviews, we found that OSA has not performed any FTE reviews or audits and reported that it did not have the resources needed to conduct these reviews.

GaDOE should formally designate personnel to be responsible for monitoring and validating the accuracy of FTE data provided by school systems. Existing personnel may be able to assume these responsibilities in addition to their current responsibilities. However, if GaDOE's current personnel do not have sufficient capacity to assume these monitoring duties, additional personnel may need to be hired. If new personnel need to be hired, GaDOE may want to consider re-establishing an FTE data auditing function where auditors conduct on-site reviews of source documentation at locations that are selected and prioritized based on risk factors. In determining the resources that should be devoted to this monitoring function, GaDOE should consider the relative costs and benefits of the activity. In addition, GaDOE should take steps to ensure that it's FTE monitoring activities are adequately documented.

GaDOE Response: *GaDOE reported that it agreed with the audit's assessment that it does not have adequate resources assigned to monitor the control activities related to its FTE data collection process. It noted that GaDOE had personnel responsible for auditing and evaluating FTE data until the previous State Superintendent of Schools eliminated these positions in fiscal year 1992. It also noted that it could not implement the recommendations suggested by the audit because it does not have staff that can take on the additional responsibility of monitoring and validating the accuracy of FTE data, and it cannot hire additional staff, given the Department's current budget crisis.*

Although state law requires that a task force be convened every three years to monitor and review instructional program cost components and funding weights used in the QBE formula, the cost components (other than salaries and benefits) have not been reviewed in more than 19 years.

OCGA 20-2-161 (f) provides for and requires that the component costs and underlying variables in the QBE instructional programs (see **Appendix C** for the Cost Categories in the High School Base Program) be periodically monitored and revised as necessary:

> *As the relative costs of the various program components will change over time and as some components will need to be added or removed, the Governor shall appoint a task force every three years for the purposes of reviewing the effectiveness of existing program weights and recommending to the General Assembly any changes needed. This task force shall be comprised of members or staff of the General Assembly, the State Board of Education, the Governor's office, and representatives of local school systems.* [5]

GaDOE personnel indicated that the last time a task force recommended changes to the component costs in the QBE instructional program was in 1990. They also reported that a task force was convened to review the component costs in 2004; however, the objectives of that task force were changed to improving the state's educational system (including developing a new cost model which was never finalized or adopted). Our review of Appropriations Acts found that since 2003 the only adjustments to the cost components (other than an insignificant increase to Medial Materials in 2007 and 2008 were to the state salary schedule and employee benefit contribution rates (e.g., Teachers Retirement System rate changes). In addition, it showed that the changes to salaries and benefits resulted from the normal budgetary process and not from any task force recommendations.

GaDOE personnel also indicated that the benefit resulting from periodic reviews of all the cost components was questionable given the limited funding available for education in recent years. In addition, it was noted that salaries and benefits make up about 84% of the total cost of all components and that those components are revised every year based on available funding.

The task force required by state law should be periodically convened as required or the law should be changed to provide for another method of evaluating the accuracy of costs used in the QBE funding formula.

[5] In 2000, the language in OCGA 20-2-161 (f) was changed from a general suggestion that the task force be convened ("may") to a requirement ("shall").

Appendix A
Objectives, Scope, and Methodology

The overall objective of this audit was to evaluate the system of controls, including both information system and business process controls, concerning the base earnings calculation of the QBE Funding Formula. The audit initially intended to focus on (1) explaining the QBE Funding Formula and process, (2) reviewing information system controls over QBE base earnings calculations, including the FTE and QBE applications, (3) reviewing business process controls for the overall QBE base earnings process, such as the monitoring of controls, (4) reviewing the three components of the base earnings calculation – FTE counts, the "base" amount, and program weights, and (5) reviewing QBE spreadsheet models used in the budget planning process for QBE. This audit was intended to evaluate controls over the QBE base earnings calculation but not to determine whether or not past base earnings were accurate.

At the outset, we intended to include an evaluation of the effectiveness of the data validation edits checks in the FTE application and the calculation business rules in the QBE application. However, work performed by our Department's information systems auditors concluded that the general, access, and security controls they reviewed were weak enough to preclude substantive testing of the edits and rules programmed in the FTE and QBE applications. Therefore, this report does not address whether these control activities are operating adequately or effectively, other than recommending that corrective action be taken to address identified problems before substantive tests can be performed.

Our Department's information systems auditors performed an information systems' internal control review and an attack and penetration assessment on the Department of Education's (GaDOE) network, applications, and IT infrastructure associated with the QBE funding formula process to identify internal control weaknesses and discover the risk of exposure to security threats and vulnerabilities. The scope of this review included IT Entity level controls, IT general controls, and assessment of internet, intranet, and web application security risks. The detailed findings and recommendations resulting from this review are contained in a "Technical Report" that was provided to GaDOE management. Due to the sensitive nature of the information, Technical Reports are considered confidential and are only provided to those with a specific business need. The report's Executive Summary, however, provides a high level overview of findings resulting from this IT internal control review and is included in **Appendix D** starting on page 24.

In planning the audit, we consulted the COSO (Committee of Sponsoring Organizations of the Treadway Commission) Internal Control framework and used COSO as a general guide in conducting the fieldwork under this engagement. The COSO framework states that internal control "is a process…designed to provide reasonable assurance regarding the achievement of objectives" in areas including financial reporting, operations, and legal compliance. COSO can also be used by auditors to assess the effectiveness of the control processes in those areas. The COSO framework has five elements:

- **Control Environment**: The "tone at the top"; management's attitude towards control.
- **Risk Assessment**: The extent to which management has identified risks and established goals or objectives.
- **Control Activities**: Actions implemented to mitigate identified risks and achieve established objectives.
- **Information and Communication**: Information flow processes and how documentation is produced and distributed.
- **Monitoring**: Management's review of the control process to assess its proper functioning.

To apply the COSO internal control framework, we obtained information through interviews with GaDOE staff as well as staffs in the House Budget Office (HBO), the Governor's Office of Planning and Budget (OPB) and the Senate Budget and Evaluation Office (SBEO). Additional information was obtained through review of available GaDOE documentation including FTE Warning Comparison records, text explanations of GaDOE business rules, FTE projection counts, FTE data procedures and QBE calculation spreadsheets. The audit focused on the most recent complete fiscal year of information available during the field work – state fiscal year 2008 – although documentation on prior years was also reviewed as necessary. We also consulted the QBE sections of the Georgia Code and reviewed general and amended Appropriations Acts as necessary.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix B
Information on the 19 QBE Instructional Programs
Fiscal Year 2008

Program	Weight in Law	FY 2008 Weight	Teacher Student Ratio	Per FTE Cost	FTE Projection	Total Cost of Program	Description
Kindergarten	1.6587	1.6556	1:15	$4,374.56	112,622	$492,671,817	Serves students in Kindergarten
Kindergarten Early Intervention Program	2.0496	2.0448	1:11	$5,402.96	12,604	$68,098,921	Serves students in Kindergarten at risk of not reaching or maintaining academic grade level.
Grades 1-3	1.2855	1.2841	1:17	$3,392.99	335,645	$1,138,840,207	Serves students in grades 1-3
Grades 1-3 Early Intervention Program	1.8029	1.7992	1:11	$4,754.10	28,527	$135,620,094	Serves students in Grades 1-3 at risk of not reaching or maintaining academic grade level
Grades 4-5	1.0323	1.0319	1:23	$2,726.54	204,124	$556,552,116	Serves students in Grades 4-5
Grades 4-5 Early Intervention Program	1.7971	1.7934	1:11	$4,738.62	16,120	$76,386,578	Serves students in Grades 4-5 at risk of not reaching or maintaining academic grade level
Middle Grades 6-8	1.0162	1.0157	1:23	$2,683.71	12,909	$34,644,004	Serves students in Grades 6-8 that are not served by the Middle Schools Program
Middle Schools 6-8	1.1213	1.1204	1:20	$2,960.37	303,796	$899,348,406	A single facility housing Grades 6-8 or 7-8; or a facility serving 6-8 and other grades but has a full-time principal serving only Grades 6-8 or 7-8
Grades 9-12	1.0000	1.0000	1:23	$2,642.32	337,318	891,301,621	Serves students in Grades 9-12
Vocational Laboratory	1.1847	1.1859	1:20	$3,133.59	73,503	$230,328,208	Provides instruction to enable students to enter the workforce or a technical institute
Special Education Category I	2.3940	2.3892	1:8	$6,312.94	15,324	$96,739,583	Serves students who have a self-contained specific learning disability or a self-contained speech-language disorder
Special Education Category II	2.8156	2.8078	1:6.5	$7,419.02	11,751	$87,180,850	Serves students with mild mental disabilities
Special Education Category III	3.5868	3.5763	1:5	$9,449.78	47,999	$453,579,881	Serves students with behavior disorders, moderate and severe mental disabilities, and specific disabilities in orthopedics, hearing, speech-language and learning
Special Education Category IV	5.8176	5.7995	1:3	$15,324.17	7,612	$116,647,381	Serves students who are deaf-blind, visually impaired/blind, profoundly mentally disabled, resourced hearing impaired and deaf, resourced orthopedically disabled and resourced other health impaired
Special Education Category V	2.4583	2.4548	1:8	$6,486.40	8,380	$54,356,011	Serves students in categories I-IV who require specially designed instruction or aids or services in alternative placements
Gifted (Special Education Category VI)	1.6673	1.6642	1:12	$4,397.32	56,825	$249,877,803	Serves students with high intellectual ability who need special instruction
Remedial Education	1.3128	1.3109	1:15	$3,463.71	10,731	$37,169,086	Serves students in Grades 6-12 who have identified deficiencies in reading, writing, or mathematics
Alternative Education	1.6025	1.5994	1:15	$4,226.16	18,640	$78,775,612	A nontraditional classroom setting for students more likely to succeed in an alternative environment (often for students with disciplinary problems)
ESOL	2.5306	2.5234	1:7	$6,667.60	13,230	$88,212,388	Serves students who score below proficiency on the English language test
TOTAL FOR ALL PROGRAMS						**$5,786,330,567**	

Note: Total cost of Program represents the total “Base Earnings” of each program
Sources: Agency Documents and State Law

Appendix C
Cost Categories for the High School Base Program
Fiscal Year 2008

COST CATEGORY	SUB-CATEGORIES		Per FTE Cost
	Description	Cost Factors	
Teachers	Base Instructional Salary[1]	$32,450.48	$1,830.29
	Retirement	9.28%	
	Medicare	1.45%	
	Health Insurance	18.534%	
	Sick Leave (8 days)	$150	
	Teacher Funded Ratio	1:23	
Counselors	10 Month Salary[2]	$41,946.78	$104.87
	Counselor Funded Ratio	1:400	
Tech Specialists	10 Month Salary[2]	$41,946.78	$38.13
	Counselor Funded Ratio	1:1,100	
Operations Direct Inst.[3]	Consumable Materials	$35.91	$98.21
	Textbooks @ 7 Years Replacement	$40.26	
	Travel	$0.93	
	Equipment Replacement	$3.11	
	Non Vocational Lab Equipment	$18.00	
Psychologists	10 Month Salary[2]	$41,946.78	$16.95
	Psychologist Funded Ratio	1:2,475	
Social Workers	10 Month Salary[2]	$41,946.78	$16.95
	Social Worker Funded Ratio	1:2,475	
Operations Central Administration[3]	Supplies	$7,818	$15.39
	Travel	$6,075	
	Equipment Replacement	$2,221	
	Misc.	$2,111	
	Unemployment Insurance & Workers' Comp.	$32,571	
	Base School System Size	3,300	
Assistant Principals	10 Month Salary[2]	$41,946.78	$86.48
	9-12 Base School Size	970	
Secretaries	Secretary (12 Months) Salary	$14,166	$29.26
	Secretary (10 Months) Salary	$11,805	
	Retirement	9.28%	
	9-12 Base School Size	970	
Operations School Administration[3]	Supplies	$2,198	$6.82
	Travel	$1,500	
	Equipment Replacement	$1,759	
	Misc.	$1,162	
	9-12 Base School Size	970	
Facility Maintenance and Operations			$298.00
20 Days Added Instruction[4]	Teacher Salary & Benefits[5]	$42,096.78	$28.22
	Teacher Instruction Days	190	
	Additonal Days	20	
	Added Instruction Funding Ratio	1:15.7	
	Additional Instruction Student Percentage	10%	
Staff Development	Base Instructional Salary[1]	$32,450.48	$16.48
	Teacher Funded Ratio	1:23	
	9-12 Base School Size	970	
	Counselor Funded Ratio	1:400	
	Technical Specialist Funded Ratio	1:1,100	
	Social Worker Funded Ratio	1:2475	
	Staff Development Calculation Percentage	0.1%	
Media Personnel	10 Month Salary[2]	$41,946.78	$43.24
	9-12 Base School Size	970	
Media Materials			$13.03
TOTAL PER FTE COST			**$2,642.32**

[1] Assumes an entry level teacher with no experience
[2] Includes base salary and employer contributions to retirement, health insurance, and medicare
[3] Most sub-categories developed by GaDOE and have no link to state law
[4] Costs associated with an extra month of classes for certain students
[5] Includes $150 for 8 additional days of instruction

Sources: Agency Documents, State Law

APPENDIX D
Executive Summary
Information Systems Control Review at GaDOE
Conducted by Department of Audits: Information Systems Audit and Assurance Division

Introduction

Department of Audits performed an internal control review and attack and penetration assessment on Department of Education's (GaDOE) network, application and infrastructure related to the QBE and FTE applications to determine internal control weaknesses and discover the risk of exposure to security threats and vulnerabilities.

This report provides a high level overview of findings as a result of Department of Audit's IT internal control review and attempts to discover and validate vulnerabilities that were considered within the review's scope. A "Technical Report" has been prepared which provides detailed findings and recommendations. The Technical Report was provided to the GaDOE in addition to this executive summary and a detailed management response is required. Due to the sensitive nature of the information, Technical Reports are considered confidential and are only provided to those with a specific business need (i.e., a "need to know" basis).

Scope

The scope of this review included IT Entity level controls, IT general controls, and assessment of internet, intranet, and web application security risks.

IT Entity level Controls

An IT control environment creates the foundation for effective IT internal control and establishes the "tone at the top" and culture of an organization. At the entity level, business objectives are set, policies are established and decisions are made on how to deploy and manage the resources of the organization. From an IT perspective, policies and other enterprise-wide guidelines are set and communicated throughout the organization. IT characteristics that may require additional emphasis are strategic alignment with the business, roles and responsibilities, policies and procedures, and technical competence. Our assessment focused on IT organization roles and responsibilities, IT risk assessment framework, and policies and procedures.

IT General Control Assessment

Our assessment of IT general controls (ITGC) are performed to determine whether management has effective IT general controls (i.e., Logical Access and Change Management) in place that help to provide reasonable assurance that application and IT-dependent manual controls continue to function effectively over time, and that the completeness and accuracy of QBE base earning calculations can continue to be relied upon once a basis for that reliance has been established. Our ITGC procedures did not include testing of the provisioning process which includes testing the process of adding, changing and deleting user access. In addition, our procedures did not include IT operational controls such as back-up and recovery, job scheduling, and incident response.

Vulnerability Assessment

Our vulnerability assessment (attack and penetration) included internet, intranet, web application and social engineering security risks associated with Department of Education's IT environments, both supporting and trusted to the QBE and FTE applications. Our assessment is performed to identify

security exposures and business risks created by internet-facing infrastructure, threats that exist within GDOE's trusted network, and web application programmatic vulnerabilities leading to potential unauthorized access. Our procedures include exploitation activities performed to validate vulnerability exposures and simulate a process that a skilled attacker would use.

Business Process / Application Controls

IT-Dependent manual controls are manual controls that depend on IT systems such as the manual review of automated reports (i.e., reconciliations, error reports). Application controls are programmed controls that apply to the processing of individual transactions and include such controls as edit checks, validations, calculations, interfaces, and authorizations. Our assessment and purpose of such controls is to provide reasonable assurance that all transactions are valid; properly authorized and recorded; and are processed completely, accurately, and on a timely basis. Specifically, over two hundred edit checks were identified related to the FTE application, including key preventive and detective controls to ensure completeness of data records as well as the identification of abnormalities requiring monitoring and follow-up. In addition, the QBE application has key "business rule" calculations, using data inputs such as FTE counts and legislative funding decisions, to perform prescribed calculations which yield QBE allotments.

Risk Analysis

The following table is an overview of finding categories for each assessment type and their associated risk ranking:

Assessment	High Risk	Medium Risk	Low Risk
IT Entity Level Control	4	0	0
IT General Control (ITGC)	6	1	1
Application Control	Not Tested	Not Tested	Not Tested
Vulnerability Assessment	7	12	16

Note: The above numbers represent categories of findings/risks and in some cases aggregate multiple instances of exceptions that occurred within each findings/risks category. Additionally, only limited IT entity level controls and ITGCs were evaluated.

Summary of Findings

The following is a summary of the identified internal control weaknesses and security issues that pose the highest risk to GaDOE.

IT Entity Level Controls

- **Unmaintained policies and procedures** - Formal IT Security and Change Management policies and procedures are not maintained, updated, or enforced. This may lead to inconsistent implementation of policies to support internal controls as well as policies that do not promote adequate IT governance.

- **Password policies not in line with best practices** - Password policies are below industry standards such as ITIL (Used by GTA), NIST and COBIT and promote a greater risk of password exploitation. In addition, there are currently competing password policies and no documented

procedure for handling lost or compromised passwords which may lead to inconsistent implementation of password configurations and password exploitation.

- **No formal IT risk assessment framework** – A formal IT risk assessment framework, such as ITIL (Used by GTA), NIST and COBIT, has not been adopted. In addition, no IT risk assessments are performed to evaluate effectiveness of IT internal controls. Lack of a formally accepted IT risk framework may lead to an inadequate alignment of IT processes and controls with the business risks and a poor implementation of IT governance.

IT General Controls

Logical Access:

- **Excessive and inappropriate administrator access** – Several users were identified to have excessive access to applications, server and databases related to the QBE and FTE applications. In addition, inappropriate access was noted creating segregation of duties issues. See change management section. Excessive or inappropriate access may lead to unauthorized access or activity.

- **Users are not appropriately identified and authenticated** - Inadequate identification and authentication controls allowed the auditors to gain unauthorized system administrator-level access to critical services, servers and databases. See Vulnerability section for additional information.

- **Inadequate password configurations** - Password settings were identified that violate GDOE's password policies. In addition, some passwords are weak, some passwords do not expire, and password reuse is not prohibited in some cases. Passwords were also found to be embedded in programs, some accounts use default passwords. See Vulnerability section for additional information.

- **No monitoring of administrator access** - User access reviews are not performed on a periodic basis to determine access is based on job responsibility. This may lead to inappropriate access retained due to job transfer or termination.

Change Management:

- **Segregation of duty conflicts** – Multiple developers were noted to have access to production environments and therefore can circumvent the change management control process. Inadequate segregation of incompatible duties may reduce or eliminate the design effectiveness of a control and can lead to unauthorized and untested changes being introduced to the production environment.

- **Change management document tool not appropriately utilized** – The change management documentation tool that provides evidence that changes are authorized, tested, and approved prior to promotion is not being utilized as intended and in line with policies and procedures. Inadequate management of this tool can lead to unauthorized and untested changes being introduced to the production environment and well as need changes not being promoted as intended.

Vulnerability Assessment

- **Insecure SQL queries allowing exposure to SQL injection** – SQL injection is a form of attack on a database-driven Web site in which the attacker executes unauthorized SQL commands by taking advantage of insecure code on a system connected to the Internet, bypassing the firewall. SQL injection attacks are used to steal information from a database from which the data would normally not be available or to gain access to an organization's host computers through the computer that is hosting the database. A SQL injection vulnerability was identified on one of GaDOE's login pages that used an insecure SQL query which did not adequately validate input data prior to processing. Using this vulnerability made it possible to bypass authentication for this particular web application. It also made it possible to view and modify entire contents of the back-end database revealing sensitive information, such as passwords and system settings. This exposure was exploited by the IT auditor to gain access to GaDOE's internal network from the Internet.
- **Local administrator passwords shared across operating system environments** – An administrator account and password was found shared on multiple operating systems across GDOE's network. Using shared administrator passwords across operating systems creates a scenario where the successful compromise of one system results in access to multiple systems on the network including production servers. This exposure was exploited by the IT auditor to gain access to critical systems.
- **Servers configured with default user name and passwords** - If a system administrator account has a default password, an intruder may gain complete control over critical services and compromise data. This exposure was exploited by the IT auditor to gain access to critical systems.
- **Sensitive data transmitted utilizing ineffective cryptographic controls** – Management of the network devices is conducted over an insecure protocol. Various server pass data between the client and server using a weak form of encryption and decryption, exposing users' credential in plain text over local and intermediate networks. This insecure protocol was noted all servers and workstations for backwards compatibility with legacy systems which compromises security. This traffic can be viewed and intercepted by malicious third parties and used to launch attacks against the application.
- **Vulnerable software versions** – Several systems were identified that were running potentially dangerous versions of software known to be vulnerable to various software exploits. A successful exploitation may result in a range of adverse consequences including buffer overflows, denial of service, and gaining administration privileges over the vulnerable systems.
- **Sensitive information stored in clear text in database** – Sensitive information was found in plain text in GaDOE's databases. Storing information in plain text in back end databases allows an attacker to directly view all unencrypted data once the database is compromised.
- **Incidents are not effectively identified and logged** - GaDOE does not have a process in place to routinely generate, store, and analyze system logs. Therefore, it may not be able to identify major security incidents, policy violations, fraudulent activity, or significant operational problems. Specifically, GaDOE has not defined the types of events that are auditable, does not have a process to routinely review log files for security anomalies, and has not investigated security violations.

Business Process / Application Controls:

Due to weaknesses in the design and the operating effectiveness of ITGCs as well as the identified security vulnerabilities within the FTE and QBE application environments, we determined that adequate IT general controls are not in place to provide reasonable assurance that application and IT-dependent manual controls continue to function effectively over time. As there is no basis that application controls can continue to be relied upon, and not modified intentionally or unintentionally, we did not perform further procedures to determine the completeness and accuracy of QBE base earning calculations. Ineffective IT controls does not preclude reliance on management's financial statement assertions, however, it does increase audit risk and therefore requires greater financial audit efforts and resources by increasing substantive testing of significant classes of transactions. In addition, it requires testing of any reliance on electronic audit evidence.

Strategic Next Steps

In addition to implementing the specific recommendations in the Technical Report, we recommend the following activities to increase the security posture of GaDOE's network and related infrastructure.

- **Address all identified vulnerabilities and perform regression testing** – After implementing the recommendations described in the Technical Report, all of the vulnerability findings should be retested to verify that security exposures have been adequately responded to and potential threats have been mitigated.
- **Develop formal server configuration and deployment procedures** – Procedures should be developed to confirm that the default configurations, passwords and mapping, as well as back-up, default, and non-essential files that might contain sensitive information, are removed from systems before they are deployed into GaDOE's network environment.

GaDOE Response: *GaDOE reported that it concurred with the finding and identified the following specific actions that it was taking to correct the issues noted by our Information Systems auditors.*

- *"Change control policies and procedures have been put into place and have been used over the past several months. Security policies and supporting standards based on GTA Enterprise Information Security policies have been written. Procedures that accompany these policies are being completed. Once the procedures are complete both the procedures and policies will be presented to GaDOE management for approval.*
- *New password standards have been created and approved by the CIO. The new standards will be presented to GaDOE management for approval.*
- *Risk management as it relates to application and system security will be managed within System Security Plans (SSP). A SSP will be developed for all GaDOE applications.*
- *An access control policy has been developed. Access control procedures have also been developed to manage user access to servers and follow the "principle of least privilege." Access to servers will now be reviewed quarterly to ensure user access validity.*
- *Server security logs are being monitored and reported to the Security Information and Event Manager (SIEM) device for alerting, monitoring, and reporting of administrative access to servers.*
- *The segregation of duty conflicts identified by the IS auditors will be mitigated by the reorganization of Technology Services and the creation of the Project Management Office (PMO). Continued review will be done to ensure that segregation of duty conflicts are mitigated to the extent possible.*

- *The administrator account cited by the IS auditors has been disabled. Administrator passwords are no longer shared across operating system environments.*
- *Servers in the GaDOE domain are no longer configured with default user names or passwords.*
- *The Telnet protocol is no longer allowed for the management of network devices. All management of network devices must be done through the Secure Shell (SSH) protocol. Static routes have been configured on all network switches that allow Simple Network Management Protocol (SNMP) access from only certain administrator consoles and deny it if attempted from all other sources.*
- *A new patch management process has been put in place to ensure the latest software versions, security and critical patches are installed in the server environments. We hope to implement regularly scheduled vulnerability assessments scans against all server systems using LANDesk Security and Patch Manager by July 2010.*
- *We are developing an incident response plan. This plan will be developed in accordance with the National Institute of Standards and Technology (NIST) 800-61 Computer Security Incident Handling Guide to address incident prevention, monitoring, detection, containment, response, recovery, and reporting. We are also developing policies and procedures for implementing a security log management infrastructure in line with the NIST 800-92 Guide to Computer Security Log Management to ensure proper collection, management, and retention of security logs."*

For additional information or for copies of this report call 404-657-5220 or see our website:
http://www.audits.ga.gov/rsaAudits/