Susan Montee, CPA
Missouri State Auditor

September 2007

ELEMENTARY AND SECONDARY EDUCATION

Data Confidentiality, Integrity and Availability

Report no. 2007-48

auditor.mo.gov

Susan Montee, CPA
Missouri State Auditor

YELLOW SHEET

Missing Security Controls Leave Confidential Data and Technology Resources Susceptible to Risk

This audit reviewed the management and control of information technology resources at the Department of Elementary and Secondary Education (DESE). Auditors found DESE and Information Technology Services Division (ITSD) management have not taken necessary steps to maintain effective controls to protect the confidentiality, integrity and availability of data and the information technology resources supporting the mission and operations of the department.

Management has not required reviews of user accounts	DESE and ITSD management do not have a process in place to perform periodic reviews of user access to data and other information resources to determine whether access rights remain commensurate with job responsibilities. As a result, terminated employees had access to DESE information technology resources, user accounts remained active after not being accessed or used for specified time periods and users have been assigned to more than one user account. Reviewing user accounts and access rights is necessary to reduce the risk that unauthorized alterations of these rights will go undetected and to ensure access rights are aligned with current job duties. (See page 6)
Security program is not fully implemented	Important security controls have not been in place because DESE and ITSD management have not fully established a security program on which department-wide security policies, standards, and procedures can be formulated, implemented, or monitored. DESE and ITSD management developed and documented certain policies for specific security controls. However, management has not completed the process of establishing and documenting policies and procedures for all key security controls nor approved all policies which have been developed. (See page 10)
Risk assessment program is not fully implemented	Identifying and assessing information security risks are essential steps in determining what controls are required and what level of resources should be expended on controls. DESE and ITSD management have not established a comprehensive risk management and assessment program. An ITSD official said DESE and/or ITSD staff perform risk assessments when developing new systems, but do not perform regular risk assessments over the entire system or network. (See page 18)
Business continuity and disaster recovery plans need to be tested	DESE and ITSD officials have documented a business continuity plan and a disaster recovery plan. However, these plans have not been tested, according to DESE and ITSD officials. Without testing the business continuity and disaster recovery plans, DESE and ITSD management cannot confirm the accuracy of individual recovery procedures and the overall effectiveness of the plans. (See page 19)

All reports are available on our website: auditor.mo.gov

Contents

Abbreviations

DESE	Department of Elementary and Secondary Education
GAO	Government Accountability Office
ITSD	Information Technology Services Division
MAEA	Missouri Adaptive Enterprise Architecture
MOSIS	Missouri Student Information System
OA	Office of Administration
SAO	State Auditor's Office

SUSAN MONTEE, CPA
Missouri State Auditor

Honorable Matt Blunt, Governor
and
D. Kent King, Commissioner
Department of Elementary and Secondary Education
and
Dan Ross, Chief Information Officer
Office of Administration, Information Technology Services Division
Jefferson City, MO 65102

The Department of Elementary and Secondary Education (DESE) is responsible for maintaining the state's public education system. DESE utilizes several web applications to calculate payments to local school districts and to track, monitor, and report school district and student information. The Office of Administration Information Technology Services Division (ITSD) is responsible for providing technical assistance to support DESE's technology resources. Our audit objective included determining whether DESE and ITSD management established adequate internal control policies and procedures and implemented effective security controls to ensure the confidentiality, integrity, and availability of data and information collected and maintained in DESE information systems.

DESE and ITSD management have not taken some of the measures necessary to maintain effective controls to protect the confidentiality, integrity and availability of data and the information and technology resources supporting the mission and operations of the department. DESE does not review or monitor user accounts which has resulted in unused and potentially unneeded user accounts. DESE and ITSD have not fully implemented security management and risk assessment programs to identify and manage security controls required to protect the department's data, systems and resources from potential threats and vulnerabilities. We found instances where critical security policies have not been developed and instances where procedures have been in place but the corresponding policies have not been documented. We also found DESE and ITSD had documented but not tested the contingency plans necessary to sustain and recover critical technology services following an emergency.

We conducted our audit in accordance with applicable standards contained in *Government Auditing Standards*, issued by the Comptroller General of the United States, and included such procedures as we considered necessary in the circumstances. This report was prepared under the direction of John Blattel. Key contributors to this report included Jeff Thelen, Lori Melton, Frank Verslues, and Amanda Locke.

Susan Montee, CPA
State Auditor

Introduction

The Department of Elementary and Secondary Education (DESE) reports to the State Board of Education and is primarily a service agency working with educators, legislators, government agencies and citizens to maintain the state's public education system. Through its statewide school-improvement initiatives and regulatory functions, DESE strives to assure that all citizens have access to high-quality public education, according to the department's website.

The scope of DESE's duties ranges from early childhood to adult education services. DESE does not regulate or evaluate private, parochial or home schools. DESE employs about 1,900 persons throughout the state and has a total budget of approximately $5 billion. The department has six divisions (1) Administrative and Financial Services, (2) School Improvement, (3) Special Education, (4) Teacher Quality and Urban Education, (5) Career Education, and (6) Vocational Rehabilitation. Almost 95 percent of the department's budget consists of state and federal funds that are allocated to local schools and other agencies.

The Office of Administration, Information Technology Services Division (OA ITSD)[1] is responsible for providing technical assistance to support DESE's technology resources. DESE maintains ownership of its information systems and data, while ITSD provides the technical support. As part of the technology support function, OA ITSD has established the Missouri Adaptive Enterprise Architecture (MAEA)[2] to guide information technology decisions. DESE is required to follow MAEA standards and policies.

DESE uses several web applications to maintain data on students and teachers and to track, monitor and record financial information. The web applications maintain private and confidential information, such as social security numbers, assessment test scores, and other sensitive information. Use of the web applications is restricted to DESE and specific non-DESE users, such as school district personnel, contractors, and other entities. Access to DESE web applications is controlled by the User Manager

[1] In this report, OA ITSD refers to the entire division, while ITSD refers to the section within OA ITSD that has been assigned specific responsibility for supporting DESE technology resources.

[2] The Enterprise Architecture includes standards, policies and guidelines established by OA ITSD. The Enterprise Architecture is made up of several information technology domains, including domains dedicated to security and information. The domains are not fully developed, but define the principles which are needed to help ensure the appropriate level of protection for the state's information and technology assets.

system. According to the DESE user manual, User Manager is designed to facilitate the administration of security throughout all of DESE web applications. Users access the main login page to login to the DESE system. After User Manager verifies user entered information, the DESE Web Application Menu page is opened. This page provides a list of all DESE web applications the specific user is allowed to access.

DESE and ITSD are responsible for maintaining the security, confidentiality and privacy of the data collected and stored in these applications. Security of information refers to protecting data from loss and unauthorized access to ensure the integrity and availability of data. Privacy of information refers to non-disclosure of information without the individual's consent and confidentiality refers to an agency's obligation to protect information obtained and not disclose information without the individual's consent, according to DESE policy.

Scope and Methodology

To determine whether DESE and ITSD management established internal control policies and procedures and implemented security controls we conducted interviews with appropriate officials and staff; requested and reviewed available policies, procedures, and other applicable information; and performed testing.

We obtained data files from ITSD of the various user accounts having access to DESE's technology resources, including specific web applications and the network, from January through March 2007. To ensure completeness of the data, we grouped the accounts by district code and briefly reviewed the codes for reasonableness.

We obtained the employment records for DESE employees and ITSD employees assigned to DESE for fiscal years 2001 through 2007 from the statewide accounting system for human resources. We did not perform specific procedures to ensure reliability because the risk of unreliable results was considered immaterial. We matched this data to the user accounts to determine if any terminated employees had active user accounts. We provided an ITSD official with a list of all terminated employees we identified.

We based our evaluation on accepted state, federal, national and international standards and best practices related to information technology security controls from the following sources:

- Missouri Adaptive Enterprise Architecture (MAEA)
- National Institute of Standards and Technology (NIST)
- U.S. Government Accountability Office (GAO)

- IT Governance Institute Control Objectives for Information and related Technology (COBIT)
- International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)

We requested comments on a draft of our report from the Commissioner of the Department of Elementary and Secondary Education and the Chief Information Officer. We conducted our work between October 2006 and May 2007.

Missing Security Controls Leave Confidential Data and Technology Resources Susceptible to Risk

DESE information technology resources are susceptible to threats and vulnerabilities including unauthorized use and disclosure of data and insufficient protection of technology assets. This situation has occurred because management had not (1) established adequate user account review processes, (2) fully implemented a security management program to provide a framework for developing controls and documenting key policies and procedures, (3) performed a risk assessment to identify possible threats and the likelihood of occurrence, and (4) tested business continuity and disaster recovery plans to ensure the availability of technology resources. Collectively, these weaknesses impair DESE's ability to ensure the confidentiality, integrity, and availability of data collected and maintained in DESE information systems and to ensure information technology resources are properly protected.

Management Has Not Required Reviews of User Accounts

DESE and ITSD management do not have a process in place to perform periodic reviews of user access to data and other information resources to determine whether the access rights remain commensurate with job responsibilities. According to the MAEA, agencies must periodically review user accounts. At a minimum, this review should include (1) levels of authorized access for each user and (2) identification of inactive, idle or orphaned accounts. Accepted standards also support regular review of all accounts and related privileges. Without a review of user access rights, there is an increased risk that unauthorized alterations of these rights will go undetected or that access rights are not aligned with current job duties. DESE and ITSD management do not have user account review processes or procedures in place to identify:

- Users with inappropriate access
- Terminated employees
- Inactive user accounts
- User accounts with no access rights
- Users with multiple accounts

Supervisors have not reviewed user accounts

According to accepted standards, there should be regular reviews of all user accounts and related privileges. DESE and ITSD management do not have procedures for supervisory reviews of user accounts. In addition, ITSD officials have not provided a list of user accounts to DESE for review or confirmation of user access rights.

We reviewed user access to specific web applications. We discussed the user's current job duties with DESE officials to determine if the access was appropriate and found 10 users no longer required access to the specific application to perform their jobs. In addition, DESE officials could not

identify five users who had access to a web application and these five users were not shown as employees in the statewide accounting system.

We also found 250 active user accounts assigned to DESE where the user has not been shown as an employee in the statewide accounting system since at least fiscal year 2001. These users could be contractors, employees terminated prior to fiscal year 2001, or other users that may or may not require access, according to an ITSD official and our review of the data. Since DESE officials have not performed periodic reviews of the user accounts, they could not determine if the access was appropriate.

ITSD sends a list of user accounts to every school district annually requesting district staff review the access of individuals in the district to the web applications. However, ITSD officials have not included comments in the accompanying letter explaining the importance of reviewing user access rights and keeping accounts accurate and current. ITSD officials have not performed any follow-up with the school districts to ensure the lists have been reviewed. An ITSD official said they do not have authority over the access provided to school district users. Although school district superintendents have responsibility for authorizing and monitoring user access for their districts, DESE and ITSD have ultimate responsibility for the security of the systems and data, according to a DESE official.

Requiring a review of all user accounts ensures the right type and level of access has been provided. Otherwise, user accounts and accesses can be granted to or maintained for users who should not have access, according to accepted standards.

Terminated employees have access to DESE information technology resources

The MAEA states agencies should have a procedure to disable user access when a user leaves employment. DESE does not have a documented policy for disabling access when users leave employment. DESE supervisors are supposed to notify the ITSD help desk when termination and transfer information becomes available, according to an ITSD official. During our review of DESE user accounts having access to any of the department's web applications, we found 162 former employees still had access, some of which included access to financial or confidential information. Unauthorized access to DESE's information resources by former employees may compromise the confidentiality and integrity of data maintained by the department.

User accounts remain active after they are no longer used

Terminating access for inactive user accounts helps prevent intruders from exploiting inactive accounts to masquerade as legitimate users, according to accepted standards. ITSD has not performed any reviews to identify user accounts that have not been accessed or used for a specified period of time.

During review of user accounts from the User Manager system, we found 6,018 (41 percent) of the 14,577 user accounts had not been accessed since 2005 or before. Of the 6,018 user accounts, 782 (13 percent) are assigned to DESE users and 5,236 (87 percent) are assigned to non-DESE users. As shown in Table 2.1, 782 DESE users have not logged into their accounts since 2005 or before.

Table 2.1: Age of Last Login to User Manager Account for DESE Users

Year of Last Login	Count	Cumulative	Percent of Total
2001	453	453	38
2002	47	500	42
2003	23	523	44
2004	107	630	53
2005	152	782	66
2006/2007[1]	401	1,183	100

[1] The user accounts last accessed in 2007 are included with 2006 because the data was obtained as of January 16, 2007.

Source: SAO analysis of DESE User Manager account access.

As noted in Table 2.2, 5,236 non-DESE users have not logged into their accounts since 2005 or before. We also identified 336 out of 1,484 institutions[3] where no user has accessed any web application in over a year.

Table 2.2: Age of Last Login to User Manager Account for Non-DESE Users

Year of Last Login	Count	Cumulative	Percent of Total
2001	1,739	1,739	13
2002	324	2,063	15
2003	426	2,489	19
2004	1,275	3,764	28
2005	1,472	5,236	39
2006/2007[1]	8,158	13,394	100

[1] The user accounts last accessed in 2007 are included with 2006 because the data was obtained as of January 16, 2007.

Source: SAO analysis of DESE User Manager account access.

User Accounts with No Access

According to accepted standards, managing user accounts involves selecting the correct access type and periodically reviewing accounts to ensure the access is correct. During our review, we identified 415 user accounts with no access to any of the web applications. The user can login to the web

[3] These institutions include public and non-public school districts, charter schools, higher education organizations, state agencies and other education institutions.

application menu page but cannot access any web applications. Since these accounts do not have access to any applications, the accounts are no longer required, according to an ITSD official. Periodic reviews of user accounts would identify if a user account is no longer required.

Users have been assigned more than one user account

Procedures are not in place to adequately track and review user accounts to identify if a user has been issued multiple accounts. Good business practices suggest limiting the number of accounts issued to a single user to facilitate user account management. We identified 201 users throughout the state who had multiple user accounts for the same school district. These 201 users had a total of 426 user accounts. Table 2.3 shows the reason there are 426 user accounts for the 201 users.

Table 2.3: Multiple User Manager Accounts

Reason for Multiple Accounts	Total
User account name did not match the user's name based on DESE naming standards	116
User account was the second (or more) account for a user	105
User account name did not match the user's name due to a name change	8
User accounts with no name	5
User accounts with no problem identified	192
Total	426

Source: SAO analysis of DESE User Manager accounts.

A user account may be reassigned to an active employee to grant additional access rights, according to an ITSD official. For the 116 cases where the user account name did not match the user's name listed in the account record, an ITSD official said terminated employee accounts may have been assigned to employees who required the same level of access. Instead of closing the terminated employee accounts and adding the access rights to the active accounts, users end up having two accounts. As shown in Table 2.3, there are 105 accounts assigned to users who already had accounts. ITSD officials said a user should only be assigned one user account for the same school district.

Network user accounts have been reviewed

An ITSD official reviewed all user accounts having access to DESE's network resources. According to this official, OA ITSD required this review for consolidation of statewide network services. As part of the review process, ITSD only retained accounts for active employees or contractors and deleted inactive accounts. We reviewed the network accounts and did not find any of the problems we found with the web application user accounts. Therefore, when DESE and ITSD have dedicated resources to reviewing user accounts, they effectively identified inappropriate accounts,

helping to reduce the risk of unauthorized access. However, without ongoing reviews of user accounts, management lacks assurance that user access will remain appropriate.

Security Program Is Not Fully Implemented

A security program provides a framework for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of an agency's security controls. A security program is the foundation of an agency's security control structure and a reflection of management's commitment to addressing security risks. According to GAO, implementing a security program is essential to ensuring controls over information and information systems work effectively on a continuing basis.

DESE and ITSD management have not fully established a security program on which department-wide security policies, procedures and controls can be formulated, implemented, and monitored. DESE and ITSD officials have developed and documented some policies for specific security controls. However, officials had not completed the process of establishing and documenting policies and procedures for some key security controls and management had not approved all policies developed. Accepted standards state policies are necessary to set organizational strategic directions for security and assign resources for the implementation of security. According to GAO, a critical element of an effective security program is developing and implementing policies and procedures to govern security over an agency's information technology environment.

DESE and ITSD need to develop policies for critical security controls

DESE and ITSD management had not established or documented policies or procedures for the following critical security controls:

- System and data ownership
- System and data classification
- Rules of behavior
- Security activity logging and review
- Segregation of duties
- Security awareness training
- Physical security

System and data owners' responsibilities need to be designated

The MAEA states information owners are necessary to administer information security. It is important to document the ownership of data and information systems because owners make decisions about classifying and protecting information and systems, according to accepted standards.

DESE and ITSD management have not documented policies identifying the data and system resource owners responsible for making decisions regarding data classification and system access. An ITSD official said staff know who

to contact for each system but agreed the detailed responsibilities of information resource owners should be formalized. Without having documented policies and procedures establishing data and information ownership responsibilities, there is an increased risk data and information resources will not be properly protected against unauthorized access.

Systems and data are not classified according to sensitivity and criticality

DESE and ITSD management do not have assurance that systems and data receive an appropriate level of protection. DESE and ITSD have not established a department-wide framework for systems and data classification, according to ITSD officials. Such a framework examines the sensitivity of both the data to be processed and the system itself to identify when to classify information as confidential, public, or other established levels, according to accepted standards.

A general classification framework is established to define an appropriate set of protection levels and the placement of data in information classes, according to accepted standards. Sensitivity is generally classified in terms of confidentiality, integrity, and availability. Factors such as the importance of the system to the organization's mission and the consequences of unauthorized use of the system or data need to be examined when assessing sensitivity. An ITSD official said ITSD personnel have been working on a classification framework and had not developed one sooner because the department was waiting for policy from OA ITSD in this area. OA ITSD issued a draft standard on data classification, but the standard had not been finalized as of May 2007.

System users are not informed of responsibilities

Accepted standards state rules of behavior should be established and made available to every user of the system. The rules of behavior should clearly delineate responsibilities and expected behavior of all individuals with access to the system. These rules should state the consequences of inconsistent behavior or noncompliance. The rules of behavior could also help ensure users are aware of applicable guidelines.

DESE has not documented the rules of behavior for department information and information systems, according to an ITSD official. Staff are informed of expected behavior informally during new hire orientation and training. An ITSD official said formal rules of behavior have not been documented because the process of informing staff of the expected behavior at training has seemed adequate.

Policies needed to log, report and review security activity

DESE and ITSD management have not taken sufficient steps to ensure system security controls have functioned properly. Policies and procedures for logging appropriate security-related events and monitoring specific access are necessary when developing effective security programs.

Accepted standards state a logging and monitoring function enables the early detection of unusual or abnormal security activity[4] that may need to be addressed to ensure the approved security level is maintained.

System security logging is available on the DESE network to identify security events. However, policies and procedures for monitoring, reviewing and investigating the logs have not been established. An ITSD official said DESE and ITSD management have never formally evaluated what needs to be logged and dedicated resources have not been available to determine what security activity needs to be reviewed.

Determining what, when, and by whom specific actions have been taken on a system is crucial to establishing individual accountability, investigating security violations, and monitoring compliance with security policies, according to GAO.

Policies needed to ensure segregation of duties

ITSD officials and staff have access to the program development, testing, and production environments. According to the MAEA, separation of duties must be established and documented so an individual does not have access to more than one critical task. Inadequately segregated duties increase the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, or computer resources damaged or destroyed, according to GAO. Although duties have been informally segregated, there has not been a formal effort to identify incompatible duties or to create a policy requiring segregation of duties among information technology staff, according to an ITSD official.

Programmers responsible for the development and maintenance of information technology resources have also been granted access to the production environment. An ITSD official said programmers' access is temporarily granted only when it is immediately necessary. However, we identified programmers whose access had not been temporary. In addition, an ITSD official said there is no monitoring or periodic review of activities performed by these programmers. Although necessary, temporary access authorizations outside of the normal scope of a user's duties should be granted sparingly and monitored carefully, consistent with the need to maintain separation of duties for internal control purposes, according to accepted standards.

[4] Security activity includes users attempting to access data they are not authorized to access, performing a task they are not authorized to perform, or accessing data they are authorized to access that is of a sensitive nature.

Employees do not receive ongoing security awareness training

Training is an essential component of a security program. Computer intrusions and security breakdowns often occur because computer users fail to take appropriate security measures. For this reason, it is vital employees using computer resources be aware of the importance and sensitivity of information they handle, as well as business and legal reasons for maintaining its confidentiality, integrity, and availability, according to GAO.

An ITSD official said personnel had not been trained on an ongoing basis regarding computer security and their roles in ensuring appropriate use of department resources. New employees receive informal security training as part of orientation and a limited number of DESE employees receive training bi-annually, but employees do not receive any other security awareness training. According to accepted standards, employees play a crucial role in helping ensure the security of computer systems and information technology resources. Accepted standards also state ongoing training programs are necessary to maintain employees' security awareness to the level required to perform effectively.

Additional physical security needed

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

DESE and ITSD management have not established adequate policies or procedures for the physical security of DESE computer facilities. ITSD has not formally established responsibility for physical security, could not provide a list of individuals with access to the computer facility and has not kept a visitor log book to track who has been in and out of the computer facility. An ITSD official agreed physical security needs to be improved but said resources had not been available. The official added the consolidation with OA ITSD should provide the resources needed to lock down the computer facility and ITSD staff area. Without ensuring the physical security of DESE computer facilities, management is unable to ensure only authorized individuals gain access to these facilities.

Documented policies are needed for established security procedures

DESE and ITSD management have established, but not documented, policies and procedures for the following security controls:

- User account management
- Network standards

- Remote access
- Computer virus controls
- Patch management
- Software licensing and use
- Review of key standards and policies

User account management policies not documented

DESE and ITSD management have not fully documented or approved user account management policies and procedures for issuing, suspending, modifying and closing user accounts. In addition, policies and procedures for the management of privileged user accounts have not been documented. ITSD has documented some basic user account administration procedures. However, these basic policies and procedures have not been approved by DESE management and have not been fully developed. According to accepted standards, user account management procedures should be established for all user accounts, including system administrators. These procedures should address all stages in the life-cycle of user access, including requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges.

DESE and ITSD management have not established procedures to ensure user access requests are appropriately authorized and retained. We found ITSD staff have not been ensuring appropriate approvals are obtained before granting access. We also found source documentation has not always been retained to support web application user access requests nor has source documentation been easily retrievable for user access requests to the network. During our review of access to the Missouri Student Information System[5] (MOSIS) web application, we found four cases where user access request forms had not been available to support the approval of the access. We also identified a network user access request that had not been approved by the user's supervisor. Officials said the method to request user access for DESE and ITSD users, including programmers, has not been standardized; phone calls, emails, or access request forms may be accepted as approval. An ITSD official said school district access approvals have not been validated because it takes too much time to ensure the individual approving the access is appropriate and ITSD does not want to be responsible for this process. This official stated the access request forms submitted to ITSD are maintained for backup in case a person had been granted inappropriate access. Access authorizations should be documented, maintained and approved, according to accepted standards.

[5] Missouri Student Information System is used to assist local schools and districts to track confidential individual student information for state and federal requirements.

Access to the MOSIS web application for school district users must be approved by the school district superintendent or an authorized representative, according to DESE policy. However, DESE has not maintained a list of individuals who may approve school district user access requests, according to a DESE official. We found two cases where the form requesting access to MOSIS had been approved by the same user being granted the access. Without ensuring access is approved by authorized individuals, users may have unauthorized access to confidential information maintained in the MOSIS application.

According to accepted standards, documented descriptions of access profiles[6] allow both administrators and supervisors to identify appropriate access privileges to provide a user. ITSD has not adequately documented access profiles that may be assigned to users for both the network and the web applications. As a result, the user access profiles may not be effectively communicated to both administrators and the supervisors responsible for granting access. An ITSD official said administrators and supervisors are aware of commonly used access profiles and are informally notified of any profiles that are not commonly used.

Without documented user account management policies, including approval and access profile descriptions, for the administration of user accounts, management cannot ensure access has been appropriately granted to only authorized individuals.

Network operation standards need to be documented

According to accepted standards, network operating policies and standards for the general control of the organization's network should be established, documented and maintained on a current basis. ITSD officials have established network operating controls for system logon, user account naming conventions, password requirements or standards, and lost or compromised passwords. While ITSD officials have established operating controls, the network operation policies and procedures have not been documented. Without documented policies and standards for general control of the network, there is an increased risk that network controls will not be applied consistently or will erode over time and not remain appropriate.

No documented policies exist for remote access to department systems

DESE management allows limited access to the department's network through remote access. The policies and procedures to control this access have not been documented. An ITSD official said very few people are allowed remote access to the network so there has not been a need to

[6] Profiles are the various roles available within each application and their respective rights, such as read-only, update, administrator, etc.

formalize the internal procedures for granting the access. According to accepted standards, as employees and organizations employ remote connectivity to corporate and government networks, the security of these remote end points becomes increasingly important to the overall security of a network. Without documented policies and procedures in place regarding methods for obtaining access to the network from outside the department, there is an increased risk of unauthorized access to DESE's information systems and data.

Computer virus control policies need to be completed and approved

The MAEA requires every state agency to have a formal virus detection policy. The goals of the virus detection policy, according to the MAEA, are to detail the procedures for preventing and managing virus outbreaks and to educate end-users about their roles and responsibilities in preventing virus outbreaks. ITSD officials have drafted a data security policy that includes a section on virus protection. This policy had not been approved by DESE management as of April 2007.

The MAEA and accepted standards require employees to be trained to know and understand safe anti-virus computing practices. However, DESE's draft policy does not include any training requirements for current employees and there is no training program to inform staff of established virus protection controls, according to an ITSD official.

Patch management procedures need to be documented

Accepted standards recommend all organizations have a systematic, accountable, and documented process for managing exposure to vulnerabilities through the timely deployment of patches.[7] According to the MAEA, patch management should include duties such as monitoring sources for vulnerabilities and threats; prioritizing and testing remediation; deploying patches; and verifying vulnerabilities have been successfully remediated. ITSD staff manage patches and officials have drafted patch management policies and procedures. However, these policies and procedures did not include all key patch management responsibilities, such as prioritizing, and verifying remediation nor have the policies been approved by DESE management. Without having a systematic, accountable, and documented patch management process for managing exposure to vulnerabilities there is an increased risk that software vulnerabilities can be exploited.

[7] Patches are additional pieces of program code developed to address problems (commonly called “bugs”) in software.

Management needs to ensure computers are reviewed for unlicensed software

DESE and ITSD officials have documented policies and procedures regarding the use of department software. However, these policies and procedures have not been approved by DESE management. The draft software use policy states software on DESE computers may only be installed and used in accordance with license agreements owned by DESE. This policy also states ITSD shall review all department computers annually for any software for which DESE does not hold a valid license. An ITSD official said the last review for unlicensed software was performed around March 2005. Without a review to ensure personal or unlicensed software has not been installed on DESE computers, management risks software license violations or possible virus threats compromising the integrity of all department systems.

DESE needs policies to review key standards and policies

The relevance of policies to support information technology strategy should be confirmed and approved regularly, according to accepted standards. According to a DESE official, an informal procedure is in place to annually validate if the policies and procedures in the administrative manual are accurate. However, these informal procedures have not been documented or formally approved by DESE management. Without documented and approved policies and procedures to guide the review process, management cannot be assured system, technological, or organizational environments are adequately addressed.

Audit Trail Logging and Monitoring Controls Are Needed

A logging and monitoring function enables the early detection of unusual or abnormal activities that may need to be addressed, according to accepted standards. Accepted standards also state that audit records should be reviewed for inappropriate or unusual activity, suspicious activity should be investigated, and appropriate actions should be taken. The MAEA states databases shall provide an audit utility to identify the user, action, time of action and object of the action to adequately track the change to the information.

DESE and ITSD management have not taken sufficient steps to log appropriate security-related events and maintain adequate audit trails for all of the department's web applications. An ITSD official said certain web applications, such as Core Data,[8] had not been designed to maintain sufficient logs or audit trails of events. Without sufficient audit trails to record appropriate events, ITSD officials are unable to adequately monitor changes to data and investigate security concerns.

[8] Core Data is used to collect and archive financial and statistical data for all school districts throughout the state. This data is used for a variety of applications including the distribution of state and federal funding to schools.

Other web applications, such as MOSIS, do maintain an audit trail and history of changes made to student data, but DESE officials have not monitored the activity or events to identify any incidents compromising security or data integrity. A DESE official said an audit trail is available if needed but this official has not seen the need to regularly monitor audit trails.

Missing Security Features Leave Confidential Data and System at Risk

Security must be considered in the design of an information system. Experience has shown it is very difficult to implement security measures properly and successfully after a system has been developed so these measures should be integrated fully into the design and development of the system, according to accepted standards. DESE and ITSD officials implemented the User Manager system without many commonly accepted security features. The system has some basic security; however, these features are inadequate and cumbersome. DESE and ITSD are implementing a new system to accommodate additional security features and expect to have the system operational by December 2007, according to an ITSD official.

The basic security features in User Manager consist of access rights granted to user accounts and passwords to authenticate accounts. However, common security features required by accepted standards are not yet available to more fully safeguard DESE web applications. Collectively, these user account and password weaknesses impair DESE's ability to ensure the confidentiality and integrity of web application data.

Logon Banners Needed

According to accepted standards, a logon banner should be used to ensure every user is notified of the proper use of the system. The MAEA requires a logon banner that notifies users, among other points, what is considered the proper use of the system, that only authorized users are to view the information maintained, and of any disciplinary action for unauthorized system usage. The DESE web applications, except for MOSIS, do not have a logon banner. A DESE official said logon banners had not been considered when developing the web applications but added it would be a good idea to have banners in place. Without a logon banner, users may not be informed or aware of the security features or the appropriate use of the program and its data.

Risk Assessment Program Is Not Fully Implemented

Identifying and assessing information security risks are essential steps in determining what controls are required and what level of resources should be expended on controls. Moreover, by increasing awareness of risks, these assessments generate support for the adopted policies and controls, which helps ensure policies and controls operate as intended, according to GAO. A risk assessment helps identify potential threats and vulnerabilities or weaknesses that could be exploited and to ensure appropriate controls are

implemented to mitigate these vulnerabilities. The MAEA also states risk assessments identify high impact assets, potential threats, and recommended controls for reducing or eliminating risk.

DESE and ITSD management have not established a comprehensive risk assessment and management program. An ITSD official said staff perform risk assessments when developing new systems, but have not performed regular risk assessments over the entire system or network. Since risks and threats change over time and employees leave, the results of risk assessments should be documented to ensure an appropriate action plan is developed to limit vulnerabilities and to reduce risk to an acceptable level.

Business Continuity and Disaster Recovery Plans Need To Be Tested

Contingency planning is designed to mitigate the risk of system and service unavailability by focusing effective and efficient recovery solutions. Ultimately, an organization would use a suite of plans to properly prepare response, recovery, and continuity activities for disruptions affecting the organization's information systems, business processes, and the facility. Plan testing is a critical element of a viable contingency capability. Testing enables plan deficiencies to be identified and addressed. Testing also helps evaluate the ability of the recovery staff to implement the plan quickly and effectively. Each information technology contingency plan element should be tested to confirm the accuracy of individual recovery procedures and the overall effectiveness of the plan, according to accepted standards.

DESE and ITSD officials have documented a business continuity plan and a disaster recovery plan. However, these plans have not been tested, according to DESE and ITSD officials. DESE's disaster recovery plan emphasizes the importance of testing plans stating, "Routine DRP [Disaster Recovery Plan] testing is critical to the success of recoverability of the agency's IT [Information Technology] operations." Without testing the business continuity and disaster recovery plans, DESE and ITSD management cannot confirm the accuracy of individual recovery procedures and the overall effectiveness of the plans. If a disaster did occur, DESE would be required to use these plans for recovery, so it is necessary to ensure the plans are adequate, feasible, and can actually be used to recover and restore information systems and information technology resources.

Conclusions

DESE and ITSD management have not taken necessary steps to fully implement effective internal control policies and procedures and effective security controls to prevent the unauthorized use and disclosure of data and to adequately protect information technology resources. DESE management does not have assurance access to data and other information resources is appropriate because periodic reviews of user accounts are not required to be performed. DESE's control environment is missing important security

components because management has not fully implemented a security program. Important security controls have not been established or have been developed but lack documented policies and procedures to provide consistent guidance. DESE and ITSD management do not have assurance appropriate controls are in place to reduce risks of threats and vulnerabilities to an acceptable level since a formal risk assessment has not been performed. The recovery of services, systems and technology resources may be delayed following a disruption in operations or a disaster since business continuity and disaster recovery plans have not been tested. Faced with the challenge of protecting systems and resources from continuing threats, vulnerabilities, and data breaches, DESE and ITSD management should support establishing and documenting the controls necessary to ensure the confidentiality, integrity, and availability of data and information collected and maintained in DESE information systems.

Recommendations

We recommend the Department of Elementary and Secondary Education management work with Information Technology Services Division officials to:

2.1 Periodically review user access to data and other information resources to ensure access rights are commensurate with user's job duties and responsibilities. DESE should work with school districts to emphasize the importance of keeping user accounts current and accurate. The reviews of user accounts should also include procedures to determine if users:

- Are current or terminated employees.
- Have an active or inactive account.
- Have an account with no authorized access.
- Have multiple accounts that are not needed.

2.2 Fully implement the department's security management program. At a minimum, management should implement security controls and document policies and procedures by taking the following actions:

- Ensure all information resources (data and systems) have an appointed owner who makes decisions about data classification and access rights.
- Establish a system and data classification framework to ensure all systems and data are classified in terms of criticality and sensitivity.
- Document rules of behavior to inform users of their responsibilities and expected behavior when using DESE systems.

- Establish and document policies and procedures to log, monitor, report, and review appropriate security activity and security violations.
- Establish and document policies and procedures to ensure adequate segregation of incompatible duties. These policies and procedures should limit programmer access to the production environment to temporary situations and ensure activity performed by programmers is periodically monitored.
- Establish an ongoing security awareness training program to communicate the security policy and to assure a complete understanding of the importance of security by all personnel.
- Establish and document appropriate physical security policies and procedures and formally assign responsibilities for physical security to ensure information systems and data are protected against unauthorized access.
- Establish where necessary and document policies and procedures for issuing, suspending, modifying and closing user accounts for both the network and the web applications, including privileged accounts.
- Document the operating policies and standards for the general control of the network.
- Document policies and procedures for granting remote access to the network.
- Complete the process of documenting and approving a virus control policy. Once the policies and procedures are approved, establish a training program to communicate the policy to all personnel.
- Document policies and procedures for patch management activities to ensure a systematic, accountable, and documented process for managing exposure to vulnerabilities through the timely deployment of patches.
- Complete the process of documenting and approving the unlicensed software policy. Ensure annual reviews are performed to identify if any software is installed without a valid license.
- Document a formal process to periodically review and re-approve key standards, directives, and policies and procedures.

2.3 Develop or acquire the functionality to maintain audit trails for logging and monitoring of appropriate web application security-related events. Audit trails already in place should be monitored and actions taken to ensure the proper functioning of controls for DESE web applications.

2.4 Implement a new system or develop additional controls for the User Manager security system that will allow management to customize and enhance security configurations.

2.5 Develop and implement logon banners for the DESE web applications to indicate the appropriate use of the applications.

2.6 Implement and document a risk assessment and management program, which includes policies, standards, and procedures for performing periodic risk assessments so management can more effectively reduce risk and protect the department's resources and its ability to perform the department's mission.

2.7 Test the business continuity plan to ensure business operations can continue in the event of a disruption to normal operations.

2.8 Test the disaster recovery plan to ensure data and systems on DESE technology resources can be promptly restored in the event of a disaster or other disruption.

Agency Comments

2.1 ITSD and DESE concur. ITSD and DESE are developing a new security system that will provide the functionality believed necessary to safeguard DESE applications and data.

2.2 ITSD and DESE concur in part. Several of the policies and procedures listed have been established. ITSD and DESE are incorporating a technology awareness program into DESE's new employee orientation program and as part of a training series for current employees. As to item (bullet) #5, ITSD is unable to segregate duties due to the number of staff and the work load. ITSD has procedures in place to monitor activity to ensure protection of the systems. Limiting access to the production environment would degrade support to DESE.

2.3 ITSD will work with DESE and take the recommendation under advisement.

2.4 ITSD and DESE concur. ITSD and DESE are developing a new security system that will provide the functionality believed necessary to safeguard DESE applications and data.

2.5 ITSD and DESE concur. This would be implemented as part of the login page.

2.6 ITSD and DESE concur. ITSD and DESE will work to assess risks and take appropriate action as determined collaboratively by ITSD and DESE.

2.7 ITSD and DESE concur.

2.8 ITSD and DESE concur.