AUDITOR GENERAL

WILLIAM O. MONROE, CPA

ORANGE COUNTY
DISTRICT SCHOOL BOARD
Information Technology Audit

SUMMARY

The Orange County District School Board (District) maintains SAP America Public Sector, Inc. (SAP) enterprise resource planning (ERP) software that provides application processing for the District's administrative systems, such as general ledger, accounts payable, purchasing, personnel, and payroll functions. Our audit focused on evaluating selected general information technology (IT) controls during the period June 2004 through September 2004 and determining whether the District had corrected, or was in the process of correcting, IT-related deficiencies disclosed by the predecessor auditor in a management letter dated October 31, 2003.

As described below, we noted deficiencies in certain general IT controls related to the District's functions and practices:

Finding No. 1: **A Districtwide security program had not been formally devised to ensure that exposures and vulnerabilities of IT resources had been sufficiently assessed by management and addressed through enforced user and system security controls. Additionally, the District had not designated a chief security officer or similar function to provide for a unified security program over the District's information resources.**

Finding No. 2: **The District lacked a formal Information Systems Development Methodology (ISDM), including written policies and procedures governing various IT functions.**

Finding No. 3: **Deficiencies were noted in the District's business continuity controls.**

BACKGROUND

SAP ERP software was operated at the District in a client-server environment. In addition, the District operated an in-house developed student application system on an IBM mainframe platform.

Both computing platforms were under the management of the Information Technology department. Information Technology is a district-level department that provides an integrated set of automated processes and support to meet the administrative and operational needs of the District. The organizational structure consists of a Senior Director and a director for each of the three sections: Technical Support Services, Customer Support Services, and Systems Development. The Senior Director reports to the Chief Operations Officer.

Finding No. 1: Districtwide Security Program

Effective security relies on a security structure that includes consideration of data classification and ownership, organizational and operational policies, a thorough review of security, user awareness, and security administration procedures. Specific procedures developed for each of the major functions of security administration include designing the security hierarchy; granting and revoking data and resource access; and reporting and monitoring activity. Also, a systematic risk assessment framework incorporates a recurring assessment of relevant information risks to the achievement of business objectives and forms a basis for determining how the risks are managed. Additionally, it is a good business practice to assign the responsibility for implementing and overseeing the security program to a chief security officer or similar function.

The absence of a Districtwide security program, the lack of, or in some instances inadequacy of, corresponding policies and procedures, along with the lack of a formally designated chief security officer or similar function, may have contributed to the following information security control deficiencies we noted at the District:

- The District had not established policies and procedures for certain security controls, such as the monitoring of user access to information resources; periodic review of user access; security administrator functions; and proper use of wireless networks, computers, keyboards, and personal digital assistants (PDAs).
- The District did not have adequate policies and procedures in place to ensure that access capabilities were timely revoked for individuals who had terminated employment with the District. The primary objective for timely revocation of system access privileges for former employees is to ensure that the privileges are not exploited by the former employees or others. Based on our testing, it was noted that nine District employees with termination dates from June 2002 through June 2004 continued to have SAP access ranging from 62 to 734 days beyond their dates of termination. Upon notification of our test results, the District indicated that it had removed the terminated employees' access. Without adequate procedures to ensure the timely revocation of access privileges for terminated employees, the risk is increased that a former employee's access privileges could be used by an unauthorized individual to make changes to data files, programs, or applications.
- The District did not follow its written procedures regarding deletion of inactive SAP accounts. Procedures had been established whereby several weekly security reports were set up to run and print automatically. One report listed users who had active accounts and inactive status. From the review of this report, personnel could make necessary deletions to accounts. Another report listed users who had active accounts without employee records, such as consultants or temporary positions. Again, this report could be used by personnel to delete accounts after review. However, the District indicated that neither of these reports was being reviewed nor were files being updated to delete applicable access.

  Procedures were also established to automatically run programs that locked accounts and deleted users who had not logged on to the system in 120 days or new users whose accounts were created but not used in 30 days. The District indicated that these programs were taken off the schedule due to performance issues. In a test of inactive user accounts, we noted that all ten of the accounts tested had been inactive in excess of 120 days. Seven of the user accounts belonged to the terminated employees discussed in the previous bullet. The number of days between the date of last log on and the date of the inactivity report from which our test was drawn ranged from 130 to 398 days. Upon notification of our test results, the District removed the inactive accounts. Without adequate procedures to ensure the timely deletion of inactive accounts, the risk is increased of possible misuse.

- The District's IT risk management process needed improvement. Risk management is the process of identifying vulnerabilities and threats to IT resources used in achieving business objectives, and deciding what measures, if any, to take in reducing risk to an acceptable level. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising District information. However, appropriate District personnel have been notified of these issues.
- Certain important security features available in the software had not been utilized, along with certain inadequate security controls protecting the network, operating system, database, and the administrative applications. Additionally, certain physical security controls needed improvement. Specific details of these security deficiencies are not disclosed in this report to avoid any possibility of compromising District information. However, appropriate District personnel have been notified of these deficiencies.
- Access authorization forms approving user access to the District's SAP applications were not on file for all users. During our testing of user access authorization, we noted that documentation of approval of SAP access was not available for 1 of the 10 users tested. Without adequate documentation of user access authorization, the level of access granted could not be verified as consistent with the access approved. When unnecessary access privileges exist, the risk is increased that unauthorized disclosure, modification, or destruction of data could occur through the misuse of the access capabilities.
- The District's monitoring of system security events and activity needed improvement. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising District information. However, appropriate District personnel have been notified of the issues.

Absent a formal security program, the risk is increased that sound information security controls will not be sufficiently assessed and imposed to prevent compromise of data confidentiality, integrity, and availability. Without the formal designation of a chief security officer or similar function, the risk is increased that the District's security program for data and IT resources will not be fully controlled and the integrity, confidentiality, and availability of information systems data and resources may be compromised.

Recommendation: The District should develop a formal security program including an assessment of defined risk, mitigating controls, and acceptance levels. Also, notification procedures and reporting tools should be enhanced to ensure that inappropriate access privileges are timely revoked and that access is properly authorized. Further, the District should designate a chief security officer or similar function and specify the duties to be performed by that person. Responsibilities should include, at a minimum: facilitating risk assessments; coordinating the development and distribution of IT security policies and procedures; and routinely monitoring compliance with these policies.

Finding No. 2: Information Systems Development Methodology (ISDM)

A formalized and documented ISDM can provide consistent guidance to all staff at all levels of skill and experience. An ISDM typically details the procedures that are to be followed when applications and systems software are being designed and developed or acquired, as well as when they are subsequently modified. Each function within an organization needs complete, well-documented policies and procedures to describe the scope of the function, its activities, and the interrelationships with other departments. Policies establish the organization's direction, while procedures indicate how policies are to be implemented and followed.

The absence of an ISDM may have resulted in the following deficiencies:

- District management had not established corresponding policies and procedures governing acquisition, installation, and authorization of application or systems software; modification and testing of systems software; the use or monitoring of File Transfer Protocol (FTP); and software and hardware performance issues and actions taken. Instead, the District used an informal and undocumented process to control its development and maintenance activities.
- The District did not have adequate policies and procedures in place to ensure proper tracking, evaluating, and application of patches and upgrades to systems software. Specific details of these deficiencies are not disclosed in this report to avoid any possibility of compromising District information. However, appropriate District personnel have been notified of these deficiencies.

Without an established methodology governing the development, maintenance, or acquisition of IT systems, management risks the successful implementation of the system and may not satisfy the users' needs or meet the organization's business needs. Also, in the absence of policies and procedures outlining controls and measures necessary for the quality and consistency with which the District's objectives are achieved, the risk is increased that management will not have a basis for determining whether directives are properly performed nor will personnel have guidelines for meeting management's expectations.

Recommendation: Management should develop and document a formal ISDM to guide the development, maintenance, and acquisition of IT systems. In particular, management should develop and distribute policies and procedures addressing the above-mentioned areas to appropriate personnel.

Finding No. 3:
Business Continuity Controls

Business continuity controls are intended to ensure continuous service to meet District business requirements, make certain IT services are available as required, and lessen the business impact in the event of a major disruption. Business continuity planning identifies and provides information on supporting resources needed and the roles and responsibilities of those involved in the recovery process, including user department personnel.

We identified deficiencies in the District's business continuity controls. Specific details of these deficiencies are not disclosed in this report to avoid the possibility of compromising District information. However, appropriate District personnel have been notified of the deficiencies.

Recommendation: The District should enhance its business continuity controls.

PRIOR AUDIT FINDINGS

The District had corrected, or was in the process of correcting, portions of the IT-related deficiencies reported by the predecessor auditor. Certain issues within Finding Nos. 1 and 3 were previously noted by the predecessor auditor and remained unresolved.

OBJECTIVES, SCOPE AND METHODOLOGY

The objectives of this IT audit were to determine the effectiveness of selected District IT controls and to determine whether the District had corrected, or was in the process of correcting, IT-related deficiencies disclosed by the predecessor auditor in the management letter dated October 31, 2003. Our scope focused on evaluating selected general IT controls during the period June 2004 through September 2004. In conducting our audit, we interviewed appropriate District personnel, observed District processes and procedures, and performed various other audit procedures to test selected IT controls.

AUTHORITY

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our information technology audit.

William O. Monroe

William O. Monroe, CPA
Auditor General

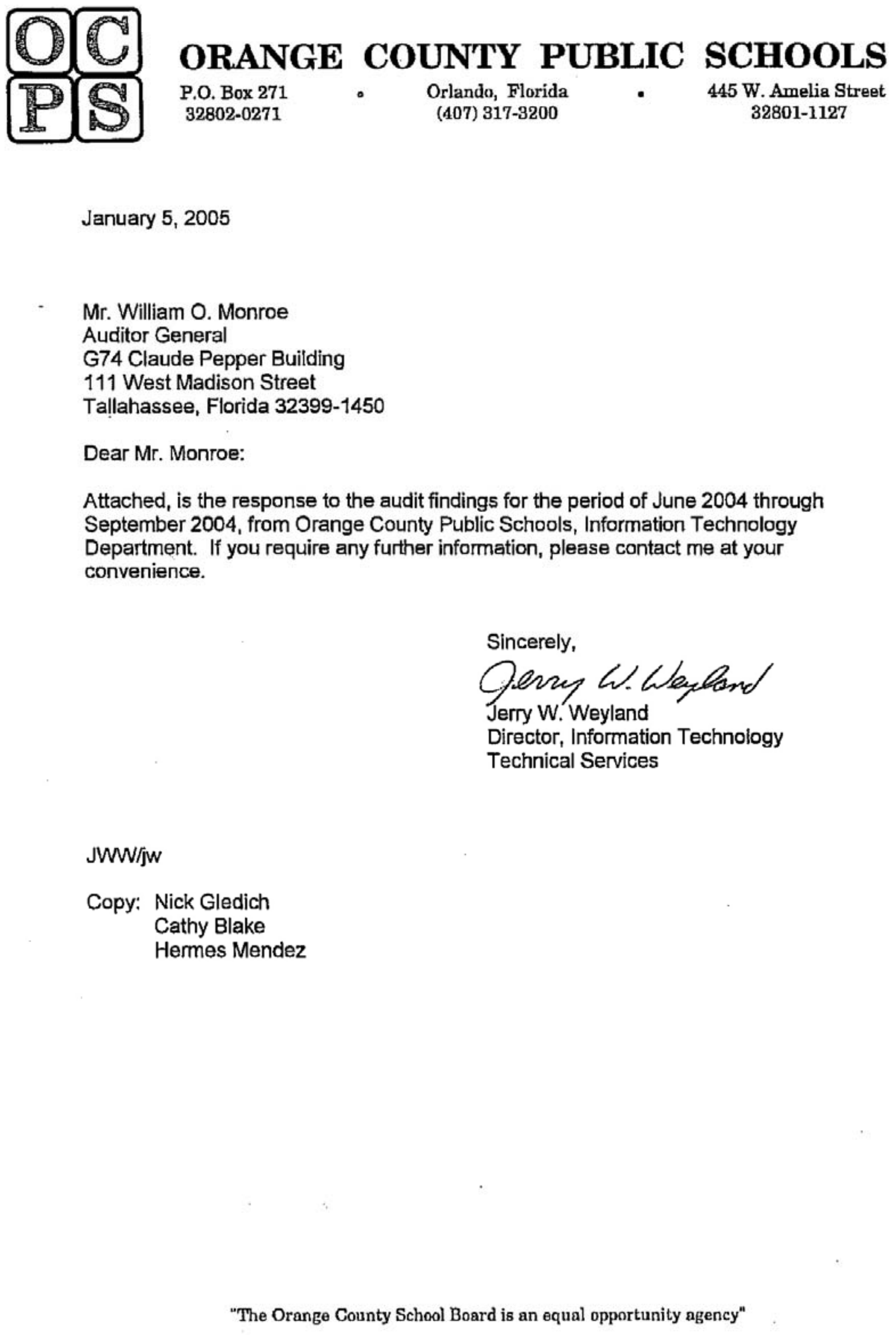
DISTRICT'S RESPONSE

In a letter dated January 5, 2005, the District provided responses to our preliminary and tentative findings. This letter is included in its entirety at the end of this report.

To promote accountability and improvement in government operations, the Auditor General makes audits of the information technology programs, activities, and functions of governmental entities. This information technology audit was made in accordance with applicable standards contained in ***Government Auditing Standards*** issued by the Comptroller General of the United States. This audit was conducted by Kathy Sellers, CISA, and supervised by Nancy Reeder, CPA*, CISA. Please address inquiries regarding this report to Jon Ingram, CPA*, CISA, Audit Manager, via e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

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

*Regulated by State of Florida.



OCPS

ORANGE COUNTY PUBLIC SCHOOLS

P.O. Box 271 • Orlando, Florida • 445 W. Amelia Street
32802-0271 (407) 317-3200 32801-1127

January 5, 2005

Mr. William O. Monroe
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Mr. Monroe:

Attached, is the response to the audit findings for the period of June 2004 through September 2004, from Orange County Public Schools, Information Technology Department. If you require any further information, please contact me at your convenience.

Sincerely,

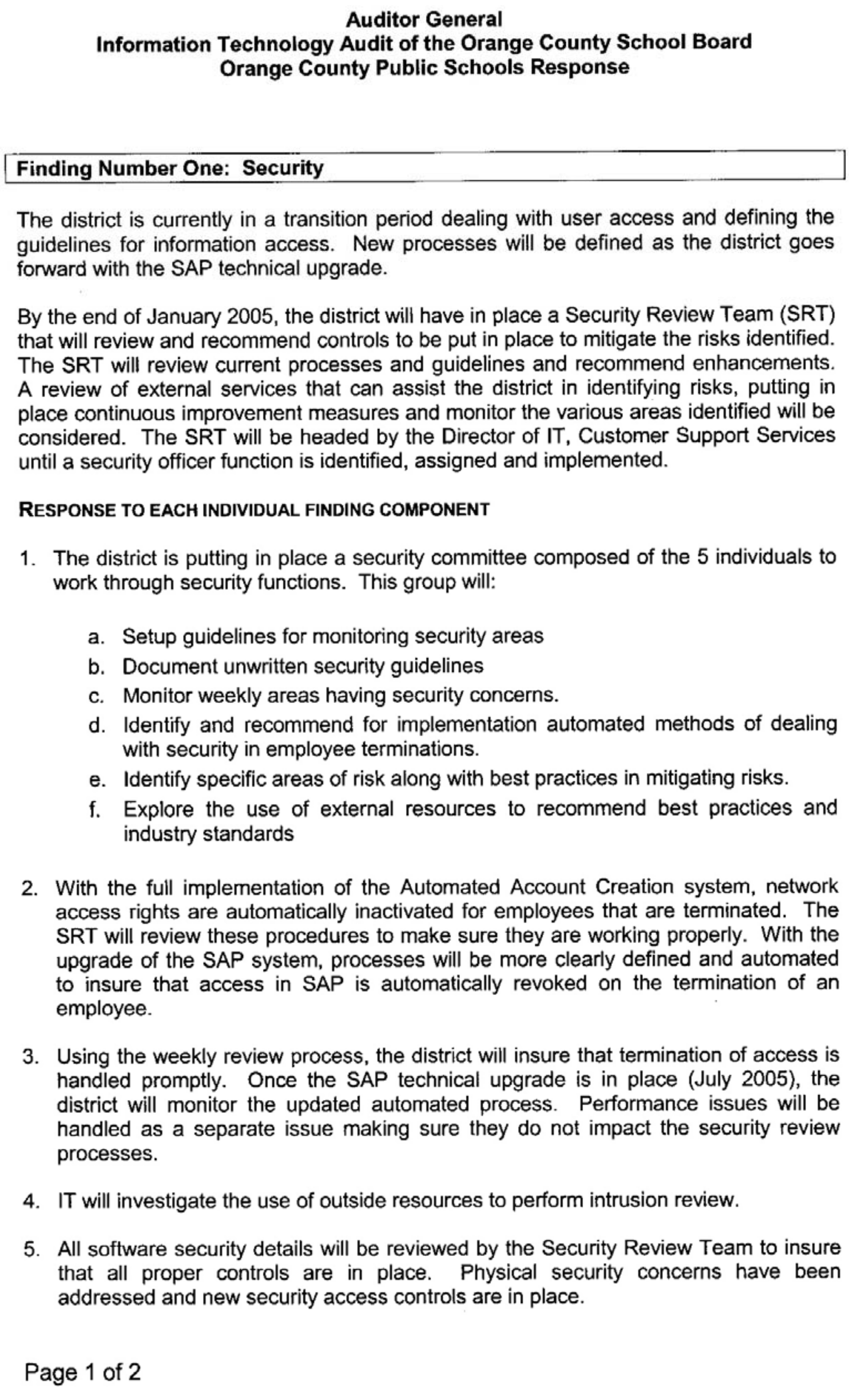
Jerry W. Weyland

Jerry W. Weyland
Director, Information Technology
Technical Services

JWW/jw

Copy: Nick Gledich
Cathy Blake
Hermes Mendez

"The Orange County School Board is an equal opportunity agency"



Auditor General
Information Technology Audit of the Orange County School Board
Orange County Public Schools Response

Finding Number One: Security

The district is currently in a transition period dealing with user access and defining the guidelines for information access. New processes will be defined as the district goes forward with the SAP technical upgrade.

By the end of January 2005, the district will have in place a Security Review Team (SRT) that will review and recommend controls to be put in place to mitigate the risks identified. The SRT will review current processes and guidelines and recommend enhancements. A review of external services that can assist the district in identifying risks, putting in place continuous improvement measures and monitor the various areas identified will be considered. The SRT will be headed by the Director of IT, Customer Support Services until a security officer function is identified, assigned and implemented.

RESPONSE TO EACH INDIVIDUAL FINDING COMPONENT

1. The district is putting in place a security committee composed of the 5 individuals to work through security functions. This group will:

   a. Setup guidelines for monitoring security areas
   b. Document unwritten security guidelines
   c. Monitor weekly areas having security concerns.
   d. Identify and recommend for implementation automated methods of dealing with security in employee terminations.
   e. Identify specific areas of risk along with best practices in mitigating risks.
   f. Explore the use of external resources to recommend best practices and industry standards

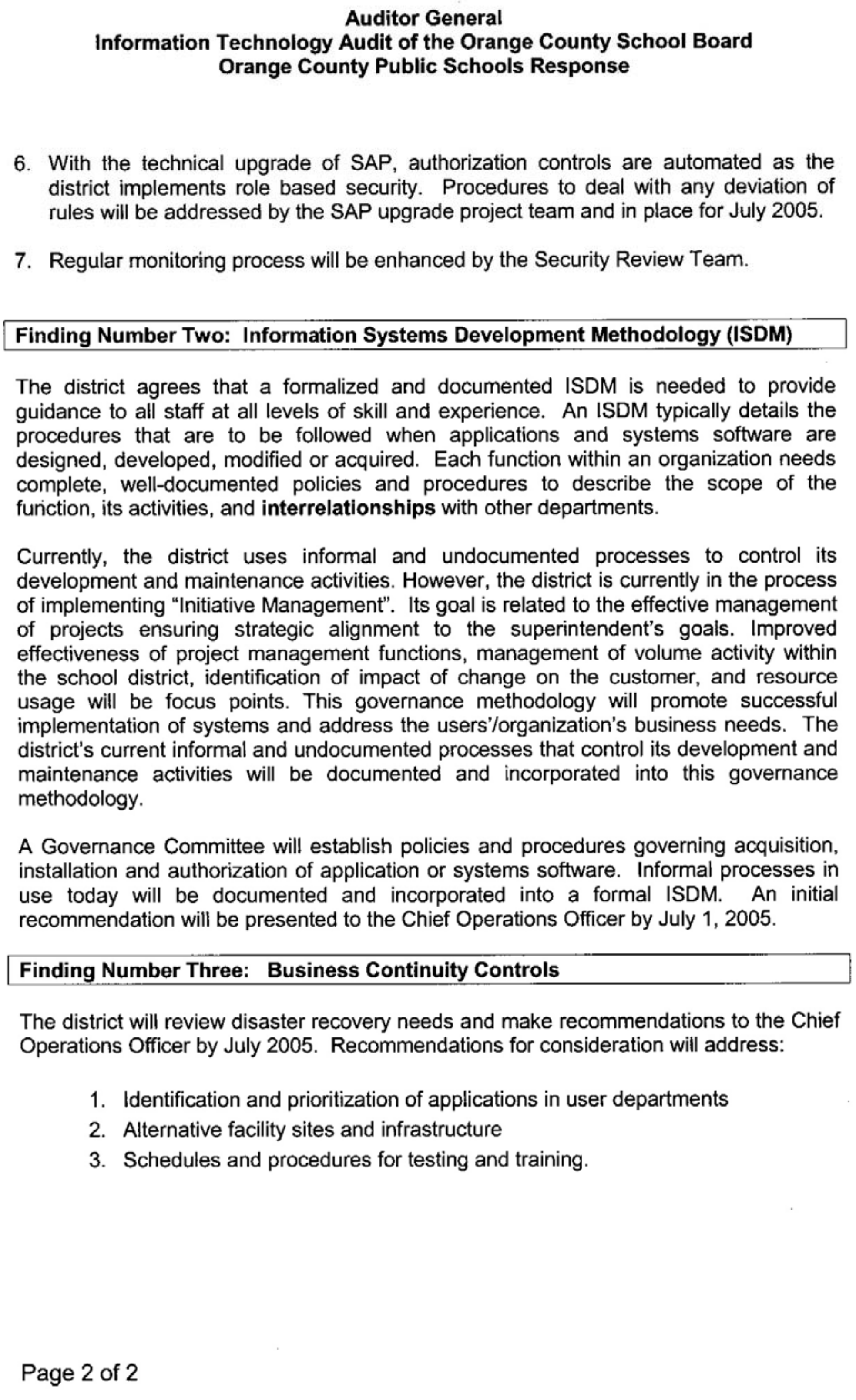
2. With the full implementation of the Automated Account Creation system, network access rights are automatically inactivated for employees that are terminated. The SRT will review these procedures to make sure they are working properly. With the upgrade of the SAP system, processes will be more clearly defined and automated to insure that access in SAP is automatically revoked on the termination of an employee.

3. Using the weekly review process, the district will insure that termination of access is handled promptly. Once the SAP technical upgrade is in place (July 2005), the district will monitor the updated automated process. Performance issues will be handled as a separate issue making sure they do not impact the security review processes.

4. IT will investigate the use of outside resources to perform intrusion review.

5. All software security details will be reviewed by the Security Review Team to insure that all proper controls are in place. Physical security concerns have been addressed and new security access controls are in place.

Page 1 of 2



Auditor General
Information Technology Audit of the Orange County School Board
Orange County Public Schools Response

6. With the technical upgrade of SAP, authorization controls are automated as the district implements role based security. Procedures to deal with any deviation of rules will be addressed by the SAP upgrade project team and in place for July 2005.

7. Regular monitoring process will be enhanced by the Security Review Team.

Finding Number Two: Information Systems Development Methodology (ISDM)

The district agrees that a formalized and documented ISDM is needed to provide guidance to all staff at all levels of skill and experience. An ISDM typically details the procedures that are to be followed when applications and systems software are designed, developed, modified or acquired. Each function within an organization needs complete, well-documented policies and procedures to describe the scope of the function, its activities, and **interrelationships** with other departments.

Currently, the district uses informal and undocumented processes to control its development and maintenance activities. However, the district is currently in the process of implementing "Initiative Management". Its goal is related to the effective management of projects ensuring strategic alignment to the superintendent's goals. Improved effectiveness of project management functions, management of volume activity within the school district, identification of impact of change on the customer, and resource usage will be focus points. This governance methodology will promote successful implementation of systems and address the users'/organization's business needs. The district's current informal and undocumented processes that control its development and maintenance activities will be documented and incorporated into this governance methodology.

A Governance Committee will establish policies and procedures governing acquisition, installation and authorization of application or systems software. Informal processes in use today will be documented and incorporated into a formal ISDM. An initial recommendation will be presented to the Chief Operations Officer by July 1, 2005.

Finding Number Three: Business Continuity Controls

The district will review disaster recovery needs and make recommendations to the Chief Operations Officer by July 2005. Recommendations for consideration will address:

1. Identification and prioritization of applications in user departments
2. Alternative facility sites and infrastructure
3. Schedules and procedures for testing and training.

Page 2 of 2