Fairfax County Internal Audit Office

Department of Information Technology
Database Administration Management Audit
Final Report

October 2009

"promoting efficient & effective local government"

Executive Summary

Much of the county's data is stored in and accessed through databases. These databases are used by critical business applications including the Sheriff's Inmate Systems (SIMS), the Fairfax Inspections Database Online (FIDO) application which supports the Department of Public Works, the Department of Planning and Zoning, the Health Department, and the Fire and Rescue Department, and dozens of additional systems. Database management systems (DBMS) are used to access the data stored in databases. Common database management systems are SQL, Oracle, DB2, and IDMS all of which are used by the county. Database administrators (DBAs) work with application developers and user agencies to maintain the databases and the database management systems throughout the lifecycle of the applications which use them. These administrators are tasked with managing the availability, reliability, security and performance of the county's databases and the database management systems. The DBA group resides within the Technology Infrastructure Division (TID) of the Department of Information Technology (DIT). They administer approximately 300 databases, up from 23 in 2001, in SQL, Oracle, DB2, and IDMS. The number of DB2 and IDMS databases is stable while the use of SQL and Oracle databases is increasing.

We found that physical safeguards to protect the hardware were in place and working effectively. Most of the databases resided on servers and on the IBM mainframe which were housed in the enterprise data center. Our primary areas of concerns were the separation of duties and supervision, audit trails, and change controls. Our findings were:

- Monitoring of DBA-level activities was not as effective as it should be since there was no independent review of DBA actions by the county's IT Security Group.
- Compliance with the portions of the county's Information Technology Security Policy 70-05.01 related to access controls and audit trail requirements needed to be strengthened. DBA level access was given to staff outside of the DBA group without the necessary oversight by senior DBA staff. Audit trails of DBA-level modifications were not consistently accessible across systems and applications.
- In several cases production data was regularly copied to development and testing databases with no masking of potentially identifying, sensitive, or confidential data.
- In regard to the SQL and Oracle databases, separation of duties among the DBA group and other DIT staff as it relates to managing the database management systems and limiting access to production data was not sufficient. We did find written documentation addressing the roles of DBAs but it lacked a detailed separation of duties discussion.
- Change management standards were not always followed when changes were made to production databases, and system or server software. For example, a change was implemented and reviewed by the same person, or a change was not documented in the Infra software which is used to track changes.

Backups of databases and software were adequate but there was no documentation of disaster recovery planning or testing for Oracle or SQL databases and servers. However, this is an outstanding finding from a previous audit (Data Center Disaster Recovery) which was performed in September 2006.

Scope and Objectives

This audit was performed as part of our fiscal year 2008 Annual Audit Plan and was conducted 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 objectives.

The scope of this audit covered the period from June 2007 through June 2008. Our objectives for this audit were:

- Determine the availability of written policies and procedures that define roles and responsibilities of the database administrators.
- Verify that database access is controlled and limited to that level necessary for users to do their job
- Confirm that audit trials are maintained and reviewed regularly
- Verify that appropriate change management controls are in place
- Verify that adequate security controls are in place and functioning
- Confirm that backup and recovery procedures exist and are tested regularly

Methodology

Our audit approach included reviewing the applicable system documentation, checking for compliance with internal county policies and procedures, interviewing management and staff of the database management group, and observing the processes used to maintain the database management systems managed by the Department of Information Technology.

Application-level controls for the systems that use these databases were not examined, as they would be reviewed as part of separate application audits. Also, databases not managed by DIT were not included in this audit. We used as references Fairfax County's Information Technology Security Policy 70-05.01 and the DIT Change Management Policy last revised in September of 2006.

The Fairfax County Internal Audit Office is free from organizational impairments to independence in our reporting as defined by Government Auditing Standards. We report directly and are accountable to the county executive. Organizationally, we are outside the staff or line management function of the units that we audit. We report the results of our audits to the county executive and the Board of Supervisors, and reports are available to the public.

Findings, Recommendations, and Management Response

1. Security Oversight

SQL and UNIX servers are used for important applications such as the Financial Accounting Comprehensive Tracking System (FACTS), Treasury Workstation (TWS), and the Sheriff Information Management Systems (SIMS) and the associated databases. The IT Security Group does not have independent access to these servers. They have to go through another group in DIT for access, and sometimes rely on another group to provide data from the servers. Without independent access, there is an increased risk to the county for fraud, undetected intrusion, or error due to the changing of data before IT Security sees it, or through the IT Security Group being given incomplete access and not seeing the whole picture. The IT Security Group cannot fully evaluate and monitor server activities, or troubleshoot potential security problems without this independent access.

Recommendation: We recommend that independent read-only access to all databases and servers be provided to the IT Security Group for the purpose of monitoring the activities of privileged accounts and troubleshooting possible security issues.

Management Response: The IT Security Group will have independent read-only access to all databases for DBProtect for the purpose of monitoring the activities of privileged accounts and troubleshooting possible security issues. The IT Security Group will create a routine procedure and conduct regularly scheduled checks on database activities. The estimated completion date is December 31, 2009.

2. Separation of Duties and Supervision

Several SQL applications used by county agencies were supported by DIT staff outside of the DBA group, who had DBA level access to the production databases and system level access to software and hardware. This condition existed on important application systems such as SIMS (Sheriff), FACTS (Budget), and several applications supporting the Department of Public Works and Environmental Services. There were also application developers in DIT with full Oracle DBA level access to production databases. One of the applications affected is Fairfax Inspections Database Online (FIDO). Broad access to production data and software with little or no monitoring and oversight may allow unauthorized changes to occur. For example, a computer programmer responsible for designing, writing, testing, and distributing Oracle program modifications who also has access to the production database content could either inadvertently or deliberately implement computer program changes that did not process data in accordance with management's policies or that included malicious code.

Separation of duties provides control by not allowing the same group or person to have the capability to perform tasks at any two of the following levels.

- User/Owner - create, modify, or delete production data
- Application Developer - modify application code
- DBA – maintain DBMS system settings or code
- System - maintain system software or hardware

Dividing duties in this manner diminishes the likelihood that erroneous or inappropriate actions will go undetected because the activities of one group or person will serve as a check on the activities of the others. Activities that involve critical or large dollar transactions or are inherently risky, such as the DBA functions, should be divided to enhance controls and be subject to extensive supervisory review.

We found little or no evidence of direct supervisory oversight of DBA actions or of DBA level tasks performed by staff outside of the DBA group. Supervisory oversight includes regular monitoring of access through audit reports, review of results of work once it has been completed, and verification that staff is adhering to county standards. This lack of oversight compounds the risks existing from the inadequate separation of duties.

In discussions with DIT management, we learned that there is consideration being given to changing the business model to put DBAs in application development groups, rather than keeping them together in a separate unit as they are currently. While this may remedy the need for application developers to have code access plus DBA level access, it could raise other issues, such as on-call coverage for database management, and control over system-wide modifications that occasionally need to be made to database management systems.

Recommendation: We recommend that DBA level access to production databases not be given to staff that also have system software level access, or application developer access. Regardless of whether the DBAs are scattered throughout the IT organization, or in a group by themselves, their work should be monitored by a qualified DBA in a formal supervisory role.

Management Response: DIT will assure that additional exceptions to policy waivers will be executed where needed. In addition, system e-mail notification processes are being implemented for the exception cases. The e-mail report will be reviewed by the associated branch manager/team lead on a daily basis. The change management numbers will be generated, along with justifications, and these processes are on file in the relevant DIT divisions.

3. Audit Trails for DBA Actions

The presence of a thorough audit trail can assist management in accomplishing security objectives including detecting violations, reconstructing events, and resolving application processing problems. The audit trail is the evidence that demonstrates how a specific
action was initiated, processed, and summarized. It should enable management to determine who performed the action, what the action accomplished, and when the action was taken. The Fairfax County Information Security Policy (PM 70-05.01) dated

October 5, 2007, mandates the use of audit logs for all confidential and sensitive data. These audit logs should include records of all modifications to the databases by the DBAs. These changes made by DBAs include modifications to the database structure, connections to other databases and/or applications, granting or removing access to tables, and adding or deleting tables.

The lack of an audit trail of these changes leaves the county vulnerable to error or fraud. For example, a change could be made to production data or to who has access to it, and then removed at a later time without anyone realizing that a change was made. At the onset of the audit, there was no efficient tool in place to provide audit data to the Internal Audit Office or to the DBA staff. However, during the course of the audit, the tool DBProtect was installed. DIT DBA staff tested the product and found that although it was installed it was not capturing all of the DBA-level changes. Work is in progress to modify the configuration of DBProtect to capture all of these changes.

Besides this general log, each application could have its own audit log depending on what was set up at application implementation. DBA-level changes to the application database such as schema changes would be captured in this log. Internal Audit found that some applications did not utilize this type of audit log.

Since DBA level changes could be captured in either of these two types of logs, depending on what action was taken, it was difficult to identify and follow an audit trail for a particular change recorded in the change management system.

Recommendation: We recommend that DBProtect be configured to produce reports of all DBA-level activities occurring on production databases and that management review them periodically (at least monthly). We also recommend that all applications containing sensitive or confidential data be required to maintain at a minimum, one week's worth of production data, database, and source code modification activity.

Management Response: The county has purchased DBProtect, a tool that will allow the auditing of Oracle databases on the enterprise servers. This software is configured to record actions by all staff with Oracle DBA privileges. Reports are produced from the audit logs and management staff reviews the reports periodically to monitor the activity. While DBProtect is being implemented, the DBA has created a read-only account for the Information Security Office to review activity. These items have been implemented.

4. Production Data Masking

The Information Technology Security Policy 70-05.01 requires that all data be classified according to specified criteria as confidential, sensitive, internal use only, and public use. In several cases production data was regularly copied to development databases with no masking of potentially identifying, sensitive, or confidential data. The Fairfax Inspections Database Online (FIDO) application and the IAS (Tax) application are both examples of applications that use this practice. Using a copy of the production database is the easiest way for application developers to be sure that they are coding and testing all possible data conditions. However, if this practice is to be used, data masking should be employed to protect all sensitive or confidential

information. The use of unmasked production data in a development, test, or training environment leaves the county vulnerable to fraud, legal consequences, and damage to the county's reputation by allowing production data to be viewed by staff not authorized to access it. The security afforded by restrictions to production data access is negated by the practice of copying to other less restrictive environments.

Recommendation: We recommend that:

1. DIT establish a standard method for data owners to communicate the classification levels of all data based on the criteria in the Information Technology Security Policy 70-05.01.
2. In all instances where production data is to be copied to any another environment, such as development, test, or training, a process be put in place to use a data masking method on data classified as sensitive or confidential.
3. For databases containing information that has not been classified based on the criteria in the Information Technology Security Policy 70-05.01, no copying of the production data should take place until such classification is completed.

Management Response: DIT will develop a process for documenting direction from data owners for the need to mask where production data is to be copied into another environment, such as development, test, or training. A process will be put in place to use a data masking method on data classified as sensitive or confidential. The above items have been implemented for FIDO. The owner agency for IAS determined that data is not sensitive and does not require masking.

5. Change Management

The changes performed by the SQL and Oracle administrators and DBAs did not always go through the county's change management process. We found records of only 16 SQL and 9 Oracle change records for the DBA group in the Infra (and Quintus) change logs for FY 2008. Further, we could not in consultation with DIT identify DB2 and IDMS changes in the Infra change request records. This indicates that only a small number of the changes were recorded. The IT Security Policy 70-05.01 requires that all changes follow the DIT change management procedures and schedule. The lack of compliance with the county's change management standard by DBAs and system administrators for database and server changes caused an increased risk to the availability and integrity of the software and data. The time required to troubleshoot a problem in a database or application is increased if a change was made to any part of the software and no documentation of the change exists. The person who made the change may not be aware that a problem exists, and therefore not be involved in the fix. Although some of the database changes are requested by the data owner or application developer, the DBA staff should not move forward with implementation until change management standards are satisfied including the creation of a change request record in Infra, the current change management reporting tool.

Recommendation: We recommend that all changes to databases and system hardware or software be performed according to the DIT Change Management Policy

and schedule or be verified through direct supervision. This will provide for independent verification of changes and assurance that no changes will be implemented without the knowledge of at least one person other than the implementer. The DIT Change Management Policy requirements include entering the information into Infra, the county's current change management reporting tool, attending the weekly change management meeting to answer any questions regarding the change, and keeping the status of the change updated in Infra.

Management Response: All the changes to databases and system hardware or software will be performed according to the DIT Change Management Policy and schedule. This includes entering the information into Infra, the county's current change management reporting tool, attending the weekly change management meeting to answer any questions regarding the change, and keeping the status of the change updated in Infra. These items have been implemented.