Fairfax County Internal Audit Office

Information Technology Security Policy Compliance Audit
Final Report
September 2007

"promoting efficient & effective local government"

Background

In April of 2003, the Department of Information Technology (DIT) published the Information Technology (IT) Security Policy. The purpose of the policy was to define the requirements for the protection of the county's information technology resources and sensitive information. The policy stated that DIT was tasked with monitoring implementation and countywide compliance with the policy. The information technology security officer (ITSO) was accountable for the development and maintenance of the IT Security Policy. In February of 2005, the county executive re-emphasized the importance of the policy and mandated compliance.

Each department director was required to assign an agency information security coordinator (AISC) who would have the responsibility to implement, administer, and monitor the policy. The department directors were ultimately responsible to see that the policy was implemented, and to ensure that all agency information technology resources were used according to laws, regulations, policies and standards. They were also charged with ensuring employee awareness of the policy and associated standards, policies, and guidelines.

Executive Summary

Our audit of Information Technology Security Policy compliance found that the level of county departmental compliance varied by department size and the experience and knowledge of individual departmental security personnel. Larger departments, including the Fire and Rescue Department, Police Department, and the Department of Tax Administration tended to be the most compliant. Compliance was less complete in the smaller departments with no existing information technology staff.

Some aspects of the security policy such as strong password usage and physical security of hardware and software were well understood and performed consistently by departments. Requirements in the policy, such as active directory user IDs and network access, were addressed by the Department of Information Technology (DIT). Others, such as change control and business impact analyses, relied mostly on the staff of individual departments to implement and monitor. There was less conformity in these areas and the level of compliance varied greatly among departments. Exhibit 1 illustrates the following areas of noncompliance by department.

- The amount of training received by the agency information security coordinators (AISCs) was not consistent. One half of the assigned AISCs have received training. There is a need for more training in a circumstance where decentralized resources are relied upon for security management.
- Twelve departments did not currently have AISCs, and seven of those had never appointed one.
- There were significant discrepancies among the departments in how AISCs were, or were not; evaluated on the duties they performed in this role. About one half of the AISCs in our sample had a job element on their evaluations that addressed their security duties and responsibilities.

- There was no process in place to document and periodically review the data backup for each application system. Eight of the ten AISCs were not familiar with the retention periods of the department's data, whether or not there were backups going offsite, or if recovery had been tested. Departments were depending upon DIT to perform the correct backups.
- One department was not encrypting confidential data when it was taken out of the office for telework.

Very little progress was made in the past four years regarding the Business Impact Analysis (BIA) and Business Continuity Plans (BCP). The AISCs needed assistance in the form of templates, instructions, and training in order to complete the BIAs and BCPs for their departments. However, the countywide continuity of operations planning (COOP) initiative has superseded the IT Security Policy and should effectively accomplish the BIA/BCP objectives.

Scope and Objectives

This audit was performed as part of our fiscal year 2007 Annual Audit Plan and was conducted in accordance with generally accepted government auditing standards. The objective of this audit was to evaluate the level of compliance with the IT Security Policy in county departments. We selected nine major areas of compliance from the policy that are identified as objectives in Exhibit 1. This audit did not examine the overall security of IT processes or components in departments' application systems, but rather the compliance with the Department of Information Technology's distributed security policy.

Methodology

We selected ten departments of various sizes, representing all deputy county executive areas within the Fairfax County government. An assessment of the level of compliance with the requirements in Fairfax County's Information Technology Security Policy was then completed for each department through interviews with the AISCs, observation of department staff, and review of documentation provided. The results were combined into a general assessment of how the county departments were doing as a whole with regard to IT security policy compliance. This report contains an aggregate of findings from all departments. Results were discussed individually with each participating department.

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. AISC Training

The training that the AISCs in the surveyed departments received was not adequate. The training that was delivered did not sufficiently cover all of the significant components of the IT Security Policy. All AISCs interviewed expressed that the training needed to be expanded and that periodic updates would be beneficial. Training began in May of 2005 as a half-day class and was planned as a quarterly class. There have been three training classes provided to AISCs, the most recent in May of 2006. Thirty-four of the sixty-eight assigned AISCs have attended the half-day training. There were also two Security Awareness Days held for all county employees at which there were breakout sessions specifically for AISCs. Adequate and timely training is necessary in order to bring all AISCs to the same reasonable level of expertise and help them to understand and learn how to perform their security role.

The Department of Information Technology is responsible for providing AISC training. Individual county departments are responsible for implementing the policy. IT security training is the vehicle for delivering security information that the departments, including managers, need to do their jobs. Training should include modules which reflect the major security issues that departments are responsible for as promulgated by the IT Security Policy 70-05.01. Organizations that develop and deliver a continuous program of training for security policy and role-based security responsibilities should have a higher rate of success in protecting information by keeping AISCs up-to-date with current practices and management expectations. Training events can also provide DIT with opportunities to evaluate the effectiveness of AISC knowledge of, and involvement in, the IT security program.

If mandatory and timely training is not provided, the AISCs may not adequately implement and monitor the IT Security Policy requirements. The risks of not improving the training are a matter of degree that does not necessarily equate to a total breakdown of security but may lead to ineffective security practices and compromised information confidentiality.

Recommendation: We recommend that:

- DIT establish initial and recurring mandatory training for all AISCs and others who play a role in IT security covering all of the IT Security Policy to include training for new AISCs as well as periodic updates. As a best practice, personnel should be required to attend training <u>prior</u> to being formally assigned as an AISC. If this is not possible, they should attend the next available training session.
- The IT Security Policy be updated to include a description of the training that DIT will provide to AISCs.
- The IT Security Policy is updated to include the training that DIT will provide for general county users, and department heads.
- Where DIT is aware of non-compliance, there should be a process in place to conduct refresher training for department staff.

Management Response: DIT currently conducts AISC training on a quarterly basis. Often due to low attendance, training has been cancelled. DIT will revamp and publish the annual schedule of training for AISCs and Agency Access Control Administrator (AACAs). This will coincide with our annual IT Security Awareness Day Activities. The anticipated completion date is October 2007. The description of training will not be in the IT Security Policy. Training content will be reviewed and published annually. The anticipated completion date is October 2007.

IT Security training is designed for all county personnel. DIT does not have training specific to department heads. We can provide general training as part of the SMT venue. The anticipated completion date is June 2008.

DIT currently recommends remedial training as a part of IT security incident response. In order to ensure training takes place, we will develop a new process that includes suspension of the noncompliant employee's access pending training based on the seriousness of the incident. The anticipated completion date is October 2007.

2. Department Participation in the Security Program

Twelve out of the sixty-eight departments/groups identified by the DIT security branch did not have assigned AISCs. Seven of those departments have never appointed an AISC.

The IT Security Policy states that each agency head should designate an Agency Information Security Coordinator (AISC) who will be responsible for developing, implementing and maintaining the Information Security Program within their agency. Agency participation in this program was mandated by the county executive in 2005.

Without the appointment of an AISC, there is no one assigned to the day-to-day monitoring of IT security policy compliance within the department.

Recommendation: We recommend that the departments who have not designated an AISC do so and that DIT schedule training for these appointees as soon as possible. The new IT security policy will contain some role definition clarifications which may help in the selection of AISCs. We further recommend that the DIT information security officer monitor departmental participation in the security program through the assignment and support of AISCs and that continued non-compliance be reported to the appropriate deputy county executives.

Management Response: The new IT Security Policy clarifies the role of the AISC for the professional/managerial duties, and establishes a new role for administrative access controls – AACA. The anticipated completion date is October 2007.

DIT will request agency review of AISC and ACCA appointments with publication of new policy and updated AISC role requirements. The anticipated completion date is October 2007.

DIT will incorporate a process for more routine reporting on non-compliance issues of basic requirements of the policy to the county executive and appropriate deputy county executive. The anticipated completion date is December 2007.

3. Application Data Backups

There was no process in place to document and periodically review the backups performed by DIT for application data. Seven of the ten department AISCs were not knowledgeable about the frequency of their critical system backups, whether or not they were taken offsite, or whether or not backups had ever been tested. Those departments were: Health Department, Office of Human Rights, Department of Vehicle Services, Police Department, Fire and Rescue Department, Office for Children, Department of Tax Administration. Most believed that the Department of Information Technology (DIT) took care of this but they were not familiar with the rules or procedures used for the process.

According to the IT Security Policy, all data should be backed up on a regular basis, the backup and recovery process should be documented, and should be tested periodically. The backup and recovery procedures should be based on business rules and a documented agreement between the data owner and the custodian. The policy requires that it should be reviewed on an annual basis.

The lack of a documented backup and recovery process could cause an incorrect backup retention schedule to be in place. If a recovery is necessary, or if another issue creates the need for prior period data, it may not be available. This could cost man hours of manual effort to recreate the data where possible, or it could cause the county to be noncompliant with state, federal, or other regulations.

Recommendation: We recommend that the Department of Information Technology develop and maintain a business process for collection, review and detailed documentation of client departments' backup agreements. This process should include: formal customer backup agreements; the required retention period and mandatory destruction rules for all of the data types; verification of DIT backups currently in place; and a schedule for periodic testing of the restore procedures.

Management Response: This will be done as part of COOP and disaster recovery planning in DIT. The anticipated completion date is December 2007.

4. Data Encryption

Unencrypted confidential data from the Office of Human Rights (OHR) was being taken out of the office (home) for telework. Case data used by the Office of Human Rights is considered confidential except to the principals of the case. Confidential information could be compromised if a diskette, compact disk, laptop, etc containing the data were to be misplaced.

All sensitive or confidential Fairfax County data must be encrypted using approved encryption techniques.

Recommendation: We recommend that the OHR

- make the implementation of encryption standards and procedures a top priority if staff will continue to be permitted to take case data out of the office,
- obtain the assistance of the Department of Information Technology (DIT) IT Security Group as necessary, and
- follow the county's teleworking standards

Management Response: No unencrypted confidential data will be allowed out of the office on any media. All electronic data uses will be accomplished through CITRIX or the appropriate federal online data base accessed only by userid and password. The anticipated completion date is June 25, 2007.

Other Audit Observations

1. **Business Impact Analysis**

The Business Impact Analysis (BIA) was either not started or not completed in five of the departments surveyed. Every department should have a BIA which includes a description of the impact that the loss of each IT application/system would have on the department's ability to continue doing business. The information gathered from the analysis and output of the BIA can be used in the development of a continuity of operations plan and organizational prioritization.

The county's continuity of operations planning (COOP) effort has taken the place of the IT Security Policy directive for a BIA. Therefore, as COOP progresses, it is expected to fully address the development of a thorough business impact analysis for each critical system. DIT will fully define its process for analysis of COOP information to coordinate, develop, and maintain a set of complete BIA material that will be used to prioritize recovery efforts.

2. Business Continuity Plan (replaced by COOP)

In six of the ten surveyed departments, the Business Continuity Plan (BCP) had either not been started or not completed. In the four years since the IT Security Policy was adopted with provisions for BCPs, virtually no actions had been taken to develop departmental plans. The departments had often not completed a BCP due to a lack of available resources, and the expressed need for more guidance on the process. This condition could negatively impact the departments' ability to recover from and continue doing business after a disaster.

Each essential (mission-critical) county information technology system, including general support systems and major applications, or grouping of like systems, should have a viable and tested BCP.

The county's continuity of operations planning (COOP) effort has taken the place of the IT Security Policy directive for a BCP. Therefore, as COOP progresses, it is expected to fully address the development of plans for each critical service and associated systems.

3. AISC Evaluations

In four of the ten surveyed departments, there were no job elements in the AISC's evaluation for rating the security duties performed. In most cases, the AISC duties were being performed by someone who was in a position for which the job description and job elements were already defined prior to the AISC appointment. The AISC tasks and responsibilities were seen as IT functions that do not fit into the job descriptions of many of those to whom they were assigned. If the tasks required of the AISC are not specifically listed and evaluated on the evaluation form, the person assigned these tasks cannot be expected to make them a priority.

This is a vital and required function in all departments and performance should be evaluated. The Department of Information Technology provides a template of duties to be added to the position description for the AISC. These duties should then be used to evaluate performance. AISC responsibilities are also described in the formal AISC appointment memo. The Department of Human Resources' interpretation of current policy was that the addition of elements to the AISC's performance evaluation be at the discretion of department directors.

County policy leaves the placement of a job element for AISC duties in the AISC's evaluation to the discretion of individual departments. However, in our opinion, DIT should continue to emphasize that departments place such an element in the assigned AISC's evaluation.