A REPORT
TO THE
ARIZONA LEGISLATURE

IT Procedural Review

Arizona Department of Administration

State Data Center

August • 2012

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

Debra K. Davenport
Auditor General

The **Auditor General** is appointed by the Joint Legislative Audit Committee, a bipartisan committee composed of five senators and five representatives. Her mission is to provide independent and impartial information and specific recommendations to improve the operations of state and local government entities. To this end, she provides financial audits and accounting services to the State and political subdivisions, investigates possible misuse of public monies, and conducts performance audits of school districts, state agencies, and the programs they administer.

The Joint Legislative Audit Committee

Representative **Carl Seel,** Chair

Representative **Tom Chabin**
Representative **Justin Olson**
Representative **David Stevens**
Representative **Anna Tovar**
Representative **Andy Tobin** (*ex officio*)

Senator **Rick Murphy,** Vice Chair

Senator **Andy Biggs**
Senator **Rich Crandall**
Senator **Linda Lopez**
Senator **David Lujan**
Senator **Steve Pierce** (*ex officio*)

Audit Staff

Joe Moore, Director and Contact Person

Melinda Gardner, Team Leader
Jay Rasband

Copies of the Auditor General's reports are free.
You may request them by contacting us at:

Office of the Auditor General
2910 N. 44th Street, Suite 410 • Phoenix, AZ 85018 • (602) 553-0333

Additionally, many of our reports can be found in electronic format at:

www.azauditor.gov

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

August 22, 2012

Members of the Arizona Legislature

The Honorable Janice K. Brewer, Governor

Mr. Scott Smith, Director
Arizona Department of Administration

Transmitted herewith is a report of the Auditor General, *An IT Procedural Review of the State Data Center, a part of the Arizona Strategic Enterprise Technology Division within the Arizona Department of Administration.* A procedural review is designed to assess, in detail, the administrative policies and day-to-day operations of an organization's IT efforts.

As outlined in its response, the Department of Administration agrees with all of the findings and plans to implement all of the recommendations.

My staff and I will be pleased to discuss or clarify items in the report.

The report will be released to the public on August 23, 2012.

Sincerely,

Debbie Davenport
Auditor General

Attachment

2910 NORTH 44th STREET • SUITE 410 • PHOENIX, ARIZONA 85018 • (602) 553-0333 • FAX (602) 553-0051

Table of Contents

Table of Contents

OVERVIEW

The Office of the Auditor General has conducted a procedural review of the State Data Center (Data Center), a part of the Arizona Strategic Enterprise Technology (ASET) Division within the Arizona Department of Administration (Department).[1] The Data Center is an essential component in the State's information technology (IT) efforts, because it supports key IT systems—such as the State's accounting and personnel systems—and because it provides IT services—in the form of technical assistance, software development, and other services—to more than 100 state agencies, boards, and commissions.

An IT procedural review is designed to assess, in detail, the administrative policies and day-to-day operations of an organization's IT efforts. It compares these policies and operations to standards and "best practices" developed by IT experts, professional groups, and industry associations. By its nature, an IT procedural review is technical, detailed, and perhaps of limited interest to someone who does not have an IT background. Nonetheless, its findings and recommendations are also relevant to decision-makers who do not have an IT background. These findings and recommendations are designed to ensure that an entity—in this case, the State—has policies and procedures in place to sustain IT operations against a variety of challenges, ranging from hackers to natural disasters, as well as making day-to-day modifications in computer systems and programs with a minimum of disruption or inconvenience to users. This report is organized to do the following:

- First, in the relatively few pages that follow in this Overview, it gives non-IT decision-makers a sense of what auditors reviewed, what was found that needs attention, and why it matters.
- Second, in the more detailed chapters that follow, it explains the issues in detail using a more technical framework that auditors believe will help the Data Center and the Department to better understand and address the issues that were found.
- Third, in the appendices, it explains auditors' review approach.

In all, this report makes recommendations in 14 areas, such as

[1] After work on this review was performed, legislation went into effect that merged the Government Information Technology Agency (GITA) and the Arizona Department of Administration's (Department) Information Services Division (ISD) and Telecommunications Program Office (TPO) into one organization, which is now known as the Arizona Strategic Enterprise Technology (ASET) office. ASET is located within the Department and is headed by a Deputy Director who also holds the title of the State's Chief Information Officer (CIO), the position formerly held by the director of GITA. The majority of the work performed for this review was done on ISD, which is now referred to within ASET as the State Data Center. The State Data Center is headed by a Chief Operations Officer (COO), who reports to the Deputy Director. The TPO is now referred to as the Enterprise Infrastructure and Communications (EIC) office.

protecting sensitive data against security vulnerabilities, ensuring that operations can be restored if a disaster strikes, and protecting against unauthorized changes in computer programs.

Information Services' Effectiveness Is Central to Data Systems and Operations Throughout the State

The Department provides an array of essential services to state government, such as human resources and employee benefits, building and planning services, motor pool, risk management, procurement, state-wide payroll and accounting. The Data Center serves as a critical element of the Department's efforts because it supports the IT infrastructure and systems upon which those services depend. It also provides IT services, such as application development, technical support, help desk, disaster recovery, database management, and information technology planning, directly to a variety of state agencies, boards, and commissions. Some of its specific responsibilities include:

- Computer operations for the State's mainframe computer, which houses critical applications such as the Arizona Financial Information System (AFIS), the official accounting system and system of record for the State of Arizona's fiscal information. Although the General Accounting Office, a Business Unit with the Department, is the owner of AFIS, and is responsible for AFIS data accuracy, the Data Center is responsible for AFIS data integrity, application support, and application modifications and enhancements.
- Processing services to many of the State's largest agencies, including the Arizona Health Care Cost Containment System (AHCCCS), the Arizona Department of Transportation (ADOT), and the Arizona Department of Revenue (ADOR), and processing of Medicaid medical claims for the State of Hawaii.[2]
- Information security services for the Department's network. The Data Center also offers security-related services, such as security assessments, to its customers.
- Disaster recovery services for the Department's systems as well as those for some of its customers.
- Computer operations and hardware support of more than 150 open system servers for the Department and 20 other state agencies.[3]

[2] Processing services refer to the operations and maintenance of mainframe, open systems servers, and related equipment and functions used by the Data Center's customers. In support of these services the Data Center is also responsible for monitoring critical systems, managing system availability, tape storage, and a variety of other things related to the IT infrastructure.

[3] Open systems refer to a class of computers and associated software that provides some combination of interoperability, portability, and open software standards that allows third parties to make products that plug into or interoperate with it, particularly Unix and Unix-like systems, such as Linux.

- End-user support services. These include troubleshooting and resolving issues for the Department and several external agencies, and helping with agencies' personal computer replacements and personal computer maintenance. Customers are often smaller agencies that have less expertise and depend on the Data Center for help.

Data Center Operations Are Deficient in Many Areas

Auditors performed an initial assessment of the Data Center's key IT-related areas of responsibility and then developed review objectives grouped into the areas of 1) data management; 2) security; 3) identity and user account management; 4) change and configuration management; and 5) policies and procedures.

As a result of the work performed on this review, auditors identified deficiencies in 14 of the areas reviewed, plus one overall concern related to IT policies and procedures. For example:

- In the data management area auditors found that the Data Center lacks a sufficient disaster recovery plan. Lack of a good plan and policies and procedures supporting the plan could result in the loss of sensitive and critical information or limit the ability to recover files or computer systems.
- In the security area auditors found that the Data Center has no documented organization-wide procedures on how risk assessments should be conducted and has not performed a risk assessment since at least 2006. Risk assessments help organizations protect sensitive information or critical IT infrastructure by avoiding or reducing security threats or identifying and implementing controls needed to protect its systems against such threats. Auditors also found that the Department's computer security awareness training policy is insufficient, does not meet state program requirements, and is not being followed consistently. Without appropriate training, employees may not be sufficiently informed about computer-related security threats and what their responsibilities are in support of the organization's security requirements, objectives, and goals.
- In the identity and user management area auditors found active user accounts linked to terminated employees, including several with remote access privileges, and one with high-level administrator access privileges to a sensitive application. Failure to remove accounts for terminated users in a timely manner could result in an increased risk of theft, manipulation, or misuse of sensitive or confidential information.
- In the change and configuration management area

auditors found that the Data Center does not have a formalized and coordinated change management process and lacks a set of effective policies and procedures to manage its efforts. Inadequate change management could lead to unauthorized changes to applications and systems and increased risk that changes will not be applied correctly and that gaps between user expectations and business requirements could occur and go undetected; and finally

- Auditors found deficiencies in policies and procedures in 12 significant IT areas. Most areas are missing approved and adopted, complete, comprehensive, up-to-date, and appropriately implemented policies and procedures. Well-documented and up-to-date policies and procedures provide staff with repeatable processes and clear expectations. Failure to clearly communicate policies and procedures could limit the accountability of staff and result in inconsistencies.

Table 1 below provides a summary of the specific areas and components of concern auditors found. It also describes the concern, provides information on its importance, and gives some examples of the problems that were identified.

Table 1 – Summary of Procedural Review Areas and Findings

Area and specific components of concern	What It Is	Why It Matters	Examples of Problems Identified
Area of concern: data management			
Disaster recovery and data backup	Policies and procedures for minimizing the probability and impact of an IT service interruption from incidents such as floods, fires, power interruptions, etc.	Insufficient policies and procedures could limit the ability to restore critical systems, result in the loss of sensitive and critical information, or limit the ability to recover files from a backup system.	• Current disaster recovery plan covers only some types of equipment. • Even for equipment covered, current plan lacks key elements stipulated as important in industry standards. • Data Center has not adequately prepared to address its responsibilities related to customer systems backup and recovery.
Identification of organization-critical or high-risk assets	The processes for inventorying network devices, services, and applications with corresponding security risk ratings and monitoring higher-risk assets for security events.	Identifying high-risk assets is necessary in order to allow an organization to define priorities and resource requirements for all of its systems and applications and as part of its disaster recovery framework.	• Data Center has not performed the work necessary to formally identify its critical assets or to document the importance and level of protection appropriate for those assets.

Area and specific components of concern	What It Is	Why It Matters	Examples of Problems Identified
Data classification	The process for labeling information to show its level of sensitivity or the degree of protection needed when handling the information.	Helps organizations categorize the information they use and maintain so that they can effectively identify the types of data that are available, where that data is located, what level of access protections are needed for the data, and whether the protections they implement meet business, statutory, or regulatory compliance requirements.	• Data Center has not yet initiated the process of identifying, inventorying, or classifying data. • The Department could be at risk of not meeting statutory requirements and failure to adequately protect sensitive information could result in financial liability and civil penalties.
Area of concern: security			
Risk assessment	The process for identifying risks such as security threats and vulnerabilities, determining the probability of occurrence, the resulting impact, and the additional security controls that would lessen this impact.	Helps organizations protect sensitive information or critical IT infrastructure by avoiding or reducing security threats or identifying and implementing controls needed to protect its systems against such threats.	• The Data Center has no documented procedures on how risk assessments should be conducted. • No risk assessments have been performed in nearly 5 years.
Security compliance	The process for ensuring that existing policies, procedures, and standards related to security are enforced and effective in complying with requirements.	Noncompliance with, or inconsistent application of, security-related policies and procedures could thwart controls established by management resulting in increased risks to systems and data.	• The Data Center does not have a formal policy, comprehensive process, or effective enforcement mechanism for security compliance; as a result, many of the Data Center's IT-related policies are not being followed throughout the entire department.
Computer security and awareness training	Actions taken to regularly inform and train staff about information security risks and their responsibility to comply with policies to reduce these risks.	Without appropriate training employees may not be sufficiently informed about computer-related security threats and what their responsibilities are in support of the organization's security requirements, objectives, and goals.	• The Department's security awareness training policy is insufficient, does not meet state program requirements, and is not being consistently followed.

OVERVIEW

Area and specific components of concern	What It Is	Why It Matters	Examples of Problems Identified
Network security	Any activities designed to protect the usability, reliability, integrity, and safety of a computer network and its data. Effective network security targets a variety of threats and stops them from entering or spreading on a network.	Effective network security protects an organization against business disruption; helps it to meet mandatory regulatory compliance requirements and to protect its data, reducing the risk of legal action from data theft; and also helps it to protect its reputation, which is one of its most important assets.	• Many of the Data Center's efforts to protect its systems are effective, but more could be done. • A large portion of the Department's network is not scanned for vulnerabilities. • Auditors identified different servers with commonly known vulnerabilities that could potentially allow attackers to appear as valid users and to view information or perform functions for which they were not authorized.
Incident response management	The process for detecting, reporting, and responding to information security incidents, such as a breach of confidential information due to a failure of IT security safeguards or computer hacking.	Without adequate incident response standards and procedures in place, as well as sufficient communication between units involved in incident response, an organization cannot ensure that incidents are responded to consistently and effectively.	• The Data Center does not have an incident response plan or policy and there is no overall oversight of incident handling.
Logging and monitoring of systems	The process for generating, transmitting, storing, analyzing, and disposing of computer security log data.	Assists in the early prevention and detection of unusual activities that may need to be addressed. Logs are also useful when performing auditing and forensic analysis, supporting internal investigations, establishing baselines, and identifying operational trends and long-term problems.	• The Data Center does not regularly monitor most logs nor does it have any formalized procedures to provide guidance on what events to look for or how often reviews should be done. • The Data Center does not have any formal follow-up procedures in place for when critical events are identified.

OVERVIEW

Area and specific components of concern	What It Is	Why It Matters	Examples of Problems Identified
Area of concern: identity and user account management			
Generic user accounts and periodic user access reviews	Identity management helps ensure that all users and their activity on IT systems are uniquely identifiable and that users' access to systems and data are in line with defined and documented business needs. Identities are enabled using authentication mechanisms, such as user accounts and passwords, and activity is controlled and monitored through both technical and procedural measures. User account management involves the policies, processes, and procedures of managing IT user accounts and related user privileges.	Generic accounts that are not assigned to a specific individual but instead used by multiple people thwart accountability and increase the risk of fraud and misuse. Periodic user access reviews help ensure that individuals with access to systems are still valid and that the type of access granted is still relevant and necessary to an individual's job requirements. Weaknesses in these areas also undermine accountability.	• The Department has some generic user accounts, including one used for a sensitive high-level administrative activity. • The Data Center does not regularly review user accounts to ensure they are still valid and the type of access granted is still relevant and necessary to an individual's job requirements. • Auditors found employees managing access to applications who were not aware of the access control policy.
Terminated employees		Failure to remove accounts for terminated users in a timely manner could result in an increased risk of theft, manipulation, or misuse of sensitive or confidential information.	• Auditors found active user accounts linked to terminated employees, including several with remote access privileges, and one with high-level administrator access privileges to a sensitive application.
Access authorization documentation		Without adequate documentation, it may be difficult for management to confirm that the access granted to its systems is appropriate and that it has been approved for all accounts.	• Almost one-third of user accounts reviewed based on a sample of 10 of the 41 user accounts created between July 1, 2010 and May 27, 2011, lacked proper documentation to substantiate appropriate authorization.

OVERVIEW

Area and specific components of concern	What It Is	Why It Matters	Examples of Problems Identified
Area of concern: change and configuration management			
Change management	The process for requesting, evaluating, approving, testing, and implementing changes to IT services with minimal disruption.	Inadequate change management could lead to unauthorized changes and increased risk that changes will not be applied correctly and that gaps between user expectations and business requirements could occur and go undetected.	• The Data Center does not have a formalized and coordinated change management process and lacks a set of effective policies and procedures to manage its efforts. • A draft policy is incomplete and fails to adequately address many of the elements defined by IT standards and best practices. • The Data Center does not maintain adequate documentation of changes made to the Department's IT systems and resources.
Configuration management	The process for establishing configuration baselines for hardware and software and developing a repository where configuration settings are stored, audited, and updated as needed.	Failure to adequately manage configurations could result in production issues or delay the resolution of issues or restoration of systems.	• The Data Center has not established a configuration management process as required by state policy.
Area of concern: policies and procedures			
Policies and procedures	Policies and procedures help ensure that an organization's IT management responsibilities are addressed and its obligations are met, provide clear guidance to employees as to what their obligations are, and demonstrate the commitment that an organization has to addressing the management of its information technology resources.	Well-documented and up-to-date policies and procedures provide staff with repeatable processes and clear expectations. Failure to clearly communicate policies and procedures could limit the accountability of staff and result in inconsistencies.	• Deficiencies were found at the Department in 12 significant IT areas. • Most areas are missing approved and adopted, complete, comprehensive, up-to-date, and appropriately implemented policies and procedures. • Even for those areas for which the Data Center has policies in place, procedures developed to support them are ineffective in achieving the desired objective. • Even policies that the Data Center has are not being effectively disseminated or communicated and key employees are not aware of some policies.

Experts, Professional Organizations, and Industry Associations Have Established a Framework for Assessing Effectiveness and Developing Solutions

Auditors make 15 recommendations to address the deficiencies previously noted. Since the services the Department offers as described earlier are not unlike those that other organizations, both within the private and public sectors, offer to their customers, the Department can draw upon existing standards, frameworks, and best practices to help them to address auditors' recommendations. In fact, these standards and frameworks exist to help organizations to define possible courses of actions or to present a preferred approach to addressing similar issues or operational challenges that they may share. Advantages to organizations exist for adopting or building internal policies and procedures based on existing standards and frameworks, such as not having to "reinvent the wheel" in developing their own sets of standards and frameworks; being able to model structures that have been proven effective; leveraging best practices developed through collective experience and knowledge; being able to share and benefit from ideas of organizations sharing like challenges; and making their operations easier to assess and audit.

In an IT services environment like the one the Department and Data Center operate in, there are a number of frameworks and standards upon which to draw.

Three of the major and generally accepted frameworks include:

- The Information Systems Audit and Control Association's "Control Objectives for Information and Related Technology," commonly referred to as COBIT. COBIT is a framework created for IT management and IT governance. It provides a process model that divides IT into four domains–Plan and Organize; Acquire and Implement, Deliver and Support; and Monitor and Evaluate–and 34 processes in line within the responsibility areas of planning, building, running, and monitoring IT operations.
- The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) publication ISO/IEC 27002, titled "Code of Practice for Information Security Management." ISO/IEC 27002 provides best practice recommendations on information security management.
- The Information Technology Infrastructure Library (ITIL), maintained by the United Kingdom's Office of Government Commerce, addresses IT service management and provides a framework for identifying, planning, delivering, and supporting IT services to an organization's business.

In addition, within specific areas, such as security, there are a number of other resources for organizations to draw upon. For example, the National Institute of Standards and Technology (NIST) publishes a series of recommendation and guidance documents, referred to as special publications (SP), covering various security-related technologies and concerns of general interest to the computer security community. One such document, SP 800-53, "Recommended Security Controls for Federal Information Systems and Organizations," contains baseline security controls that organizations can use to help them to select and specify security controls for information systems. NIST is also responsible for the Federal Information Processing Standards (FIPS), which are binding on federal agencies.

In the course of this review, auditors referenced some of the above resources. Additional information about how this type of information was used can be found in the Appendix, pages 45 through 46.

Detailed Chapters Aimed at Providing a Roadmap for Information Services

The chapters that follow contain auditors' detailed findings and recommendations. The information is intended to assist the Data Center and the Department to fully understand the basis of auditors' conclusions and to provide them with some specific information to help them address the problems found. For example, auditors provide detailed descriptions of IT standards and best practices for a number of areas as potential models that the Data Center can use when developing their own strategies to address the problems that were discovered.

The report also reflects a common reason that the Data Center and Department cited for the problems that auditors found, namely resource restrictions, primarily related to budget and staffing limitations. Although auditors did not validate these claims in every case, auditors noted that as of July 2011, the Data Center had 163 authorized positions with 47 vacancies, a vacancy rate of nearly 29 percent. In some areas, such as the Data Center's compliance unit, auditors noted that the Data Center was authorized for three positions but two positions had been vacant since August 2009 and during the course of the review, the only compliance unit employee on staff had resigned and the position had yet to be replaced.

Although staffing and resource requirements may be a factor contributing to the number and types of findings auditors discovered, they are not the only factors and the Data Center and

Department still have a number of options to begin to address the problems found. In cases where budget and staffing continue to be concerns, the Data Center and Department could better assess the impact those factors have on its ability to provide required services and could develop business case assessments and justifications for policymakers to use when considering requests for additional resources.

CHAPTER 1: DATA MANAGEMENT ISSUES

According to the Data Management Association International, data management is the development, execution, and supervision of plans, policies, programs, and practices that control, protect, deliver, and enhance the value of data and information technology assets. Data management requires identifying and categorizing data as well as protecting IT resources in which data is housed. An effective data management process consists of minimizing interruptions to the availability of data, procedures for backup and recovery of data, inventorying IT assets, and labeling information to show its level of sensitivity based on confidentiality, integrity, and availability requirements relevant to all stakeholders.

Auditors' evaluation of data management practices identified deficiencies in the areas of disaster recovery and data backup, identification of organization-critical or high-risk assets, and data classification. Specifically:

- The Data Center does not have a current, complete, comprehensive, and well-documented IT disaster recovery plan; its disaster recovery testing processes are insufficient; it has not adequately prepared to address its responsibilities related to backup and recovery services offered to its customers; and it does not maintain a prioritized list of customer systems to use in the event of a disaster.
- The Data Center does not have a sufficient process for identifying and monitoring organization-critical or higher-risk assets.
- The Department does not have a complete, implemented, organization-wide data classification process, which could hinder its ability to monitor or prevent unauthorized access, modification, disclosure, or destruction of sensitive data and could result in the Department's failure to meet statutory requirements or cause it to incur financial liability or civil penalties.

Disaster Recovery Plans and Delineation of Related Responsibilities Are Incomplete

IT standards and best practices provide guidance on the types of factors that should be considered when developing a disaster recovery plan for Information Technology. They also spell out the components of such a plan. The Data Center, however, lacks a comprehensive and documented IT disaster recovery plan. The documents it has do not contain the key elements of such a plan. Also, the documents it has do not address all the systems the Data Center maintains, and it has not adequately prepared to address its responsibilities to its customers.

Disaster recovery planning is important–Disaster recovery planning is an especially critical business requirement for organizations, like the Department, that are heavily reliant on technology and the data processed by its electronic systems. A properly considered, current, and well-documented disaster recovery plan minimizes the likelihood and impact that a major IT service interruption will severely affect key business functions and processes. For the Department, such a plan is particularly important because it is responsible for several large and critical state-wide IT systems, such as AFIS, the State's accounting system, and the Human Resources Information System (HRIS), the State's personnel system. The Department also offers a variety of IT hardware- and software-related services to other state agencies. Failure to establish and test a disaster recovery plan could limit the Department's ability to restore critical systems and network components and recover electronic data files from backup files, and could result in the loss of sensitive and critical systems or data.

IT Standards and Best Practices Call for Disaster Recovery Plans to Include Number of Key Elements

Key factors for disaster recovery planning described–Benchmarks for an effective, comprehensive plan are available from IT-related standards and best practices. Such a plan would need to consider a number of key elements, such as:

- Regulatory requirements–There may be state or federal requirements for disaster recovery that need to be considered and met.
- Strategy and policy–The disaster recovery plan needs to take into account the objectives and requirements of the organization's overall business continuity plan. Policies that drive disaster recovery efforts need to be established.
- Asset management–A critical first step in developing a plan is identifying and maintaining an accurate database of IT assets. Information on server names and configurations, and existing applications, is particularly relevant and needs to be kept up to date to be of value.
- Application analysis–In addition to identifying applications and the equipment they run on, it is also important to understand the interdependencies between the applications and to involve the relevant parties in the disaster recovery planning process.
- Change management–The change management process supports both operational and disaster recovery requirements. It is important to consider the impact changes to servers and applications may have on disaster recovery efforts.

- Business impact analysis–An analysis of the potential impact that loss of IT resources and applications may have on the organization must be performed.
- Risk assessment–Assessment of the risks, both internal and external, that organizations face, and identification of gaps between risk and current practices help point out exposures that may impact business operations and would need to be mitigated.
- Emergency response–Emergency procedures need to be defined and communicated to those responsible for disaster recovery.
- Data storage integration–Solutions need to be established to manage the critical systems and their data. Considerations for data availability need to be addressed, including requirements for the amount of data that can be lost from the point of failure to the point of recovery and the time frame within which it must be recovered.
- Integration between business continuity and disaster recovery planning–IT disaster recovery requirements must reflect business needs. Involvement of business users in disaster recovery planning is required to ensure that business needs are properly identified and met.
- Building, maintaining, and testing plans–Effective plans are documented and include a great deal of information that must be maintained and tested on a regular basis. Changes need to be made to the plan as the environment changes and as testing identifies deficiencies that need to be addressed.
- Establishment of business processes to support disaster recovery efforts–A business process, supported by upper management, needs to be established to ensure that disaster recovery efforts continue to meet business requirements and are effective.

Main components of plan identified–Further, the National Institute of Science and Technology identifies five main components of a contingency plan,[4] as follows:

- Supporting Information–Provides essential information to ensure a comprehensive plan, such as a business impact analysis, points of contacts lists, and procedures.

[4] National Institute of Science and Technology Special Publication 800-34 Rev. 1, "Contingency Planning Guide for Federal Information Systems," May 2010. Information system contingency planning represents a broad scope of activities designed to sustain and recover critical system services following an emergency event. It fits into a much broader security and emergency effort that includes organizational and business process continuity, disaster recovery planning, and incident management. 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, mission/business functions, personnel, and the facility. Contingency planning normally applies to information systems, and provides the steps needed to recover the operation of all or part of designated information systems at an existing or new location in an emergency.

- Activation and Notification Phase–Includes activation criteria, notification procedures, and an outage assessment, which is used to assess the nature and extent of the disruption.
- Recovery Phase–Identifies the sequence of recovery activities, recovery procedures, and escalation and notification requirements.
- Reconstitution Phase–Defines the actions taken to test and validate system capability. Addresses concurrent processing requirements, testing, notifications, cleanup, offsite data storage, backup, and documentation.
- Appendices–Key information not otherwise included in the main body of the plan, such as vendor contact information, detailed recovery procedures and checklists, system interconnection information, reciprocal agreements with other organizations, and so on.

In addition, IT best practices and standards indicate that a comprehensive disaster recovery plan would include various procedures including those for escalation, prioritized recovery strategies, temporary operation, IT processing resumption, maintenance, testing, plan awareness and training, regulatory requirements, contact information, alternate processing facilities, and alternate suppliers for critical resources. IT standards and best practices also provide guidance on testing of disaster recovery plans indicating that testing should be done on a regular basis, cover realistic scenarios, and be based on established recovery priorities, and that the results should be reported.

Existing Plan Lacks Comprehensiveness

Despite the fact that the Department is responsible for some of the most critical IT systems in the State, and provides IT services to other organizations, including many other state agencies and the State of Hawaii's Medicaid-type system, the Data Center does not have a comprehensive and documented IT disaster recovery plan that covers the parts of those systems for which the Data Center is responsible.[5] It does, however, perform many tasks requiring effective disaster recovery efforts. Those tasks are separated into two areas corresponding to the major IT system processing platforms the Data Center maintains, namely mainframe and open

[5] Application owners, such as those accountable for HRIS, for example, are responsible for preparing disaster recovery plans for their specific applications or systems. In such cases, they would still be dependent upon the Data Center's efforts because the Data Center is responsible for the hardware and infrastructure components upon which those applications run and thus the application owners would be impacted in the event of a major disruption to those components,

systems.[6] Mainframe refers to all systems, data, and customers residing on the Data Center's large mainframe computer, while open systems refers to all systems, data, and customers residing on the other various servers housed by the Data Center. The Data Center would also be responsible for network infrastructure components, such as internal routers and switches, which support those environments.

Existing planning is incomplete–Although the Data Center was able to provide some documents related to disaster recovery planning it had done for mainframe systems, these documents were incomplete in a number of respects. For example, the Data Center supplied an Interagency Service Agreement between the Department and another agency, which describes their joint responsibility to develop and maintain an "Emergency Contingency Plan" to ensure continuity of operations in the event of disaster or disruption to normal services. The purpose of this plan is to outline the reciprocal agreement between the two agencies to back up each other's mainframe data, with the intent of being able to restore operations from their respective sites in the event of a disaster. However, auditors' review of the plan found that it lacked detail and appeared to be incomplete. For example, the document supplied was a draft from 2009 and did not contain a current list of contacts, and the procedures for recovery operations was not comprehensive, consisting only of a bulleted list of 10 abbreviated steps. The Data Center also provided a disaster recovery testing document for its mainframe systems. However, none of these documents contained all the key elements and components of a disaster recovery plan as previously described. Instead, these documents covered only a small subset of the information and procedures that would be needed in the event of a major disruption or disaster.

No planning documentation exists or testing done for open systems–Further, the Data Center did not have any disaster recovery planning documentation for the open systems area and the Data Center had not performed any disaster recovery testing on its open systems. According to the Data Center, many of its customers in its open systems environment would be responsible for their own disaster recovery planning, unless they specifically contracted with the Department to perform that service. However, as noted earlier, since the Data Center is primarily responsible for maintaining the hardware and infrastructure for many of those

[6] Open systems refer to a class of computers and associated software that provides some combination of interoperability, portability, and open software standards that allows third parties to make products that plug into or interoperate with it, particularly Unix and Unix-like systems, such as Linux. As described here, the open systems the Department maintains refers to all servers and the applications they house that the Data Center has responsibility for, which include over 150 servers for the Department and 20 other state agencies. These include servers located both in the Department's data center and at remote customer sites.

systems, the Department still has a responsibility to plan for disruptions to that environment, particularly for those events that are outside of its customers' control.

Data Center not adequately prepared to address its customers' requirements–Additionally, auditors found that the Data Center has not adequately prepared to address its data backup and disaster recovery responsibilities for those customers who have contracted with the Data Center for these specific services. For example, the Data Center provides data backup and recovery services to customers on a contract basis; otherwise, customers are responsible for performing their own backup and recovery activities. However, after multiple attempts to obtain a list of customers and their backup and recovery requirements, auditors concluded that the Data Center does not regularly maintain a comprehensive list of what disaster recovery or data backup services it is supposed to provide to its customers who have contracted for these specific services. Having an up-to-date list is important because in the event of a disaster the Data Center may not be able to compile the list in a timely enough manner to ensure that it is providing the right services to its paying customers and sufficiently meeting their needs.

In addition, the Data Center does not have a prioritized list of mainframe or open systems that would be needed in the event of a disaster. Such a list would help to ensure that systems receive attention in relation to their overall importance to state business and operational requirements. For example, if a major disruption or disaster were to occur, the order in which systems were restored may not match the criticality or operational priorities of its customers or the State. Further, the Data Center may restore equipment and services it maintains without proper regard to the customers it has contracts with as opposed to other customers who use its equipment and services but for which the Data Center does not have such an arrangement.

Finally, since many of the Data Center's customers are smaller agencies with less sophisticated IT knowledge, experience, or staff, some of these agencies may be at increased risk if they need to recover from system disruptions or disasters. It may also be unclear to these agencies what their responsibilities are and what services the Data Center is performing for them. For example, the Data Center indicated that some of its open systems customers might incorrectly assume that the Department's data center will provide full off-site backup and disaster recovery services for them. However that is not the case unless those customers specifically contract for those services. Although the Data Center indicated that it was unaware of what some of their customers' backup strategies were, they acknowledged that they knew of at

least one customer who did not run its own backups nor use the Data Center for these services. The Department attempts to specify each party's responsibilities in its contracts, but better and more frequent communication about each party's responsibilities may be required to ensure that state services are not unnecessarily affected.

Data Center agrees that existing documentation and plans are lacking–The Data Center agreed that it was lacking documentation for many areas related to disaster recovery including current, complete, and comprehensive disaster recovery plans for its systems. It indicated that a recent management change has caused delays in working on disaster recovery preparedness and that it has not had enough time or other resources available to address all the gaps in its disaster recovery process.

Recommendation 1.1

A. The Department should:
    a. Create and finalize a comprehensive disaster recovery plan, which includes all system and infrastructure components for which it is responsible, and addresses important elements such as regulatory and contractual requirements, the Department's overall business continuity needs, IT resource management requirements and interdependencies, an analysis of business impacts, risk assessments, emergency procedures, testing, and ongoing maintenance of its disaster recovery efforts.
    b. Formally document and publish the plan. The plan should include information related to the activation and notification, recovery, and reconstitution phases, and should include supporting documentation.
    c. Test the plan on a regular basis using realistic scenarios, as defined in the plan, and document and make modifications when necessary to correct any problems identified through testing.

B. The Data Center should establish formal procedures and benchmarks to ensure that customers who contract with it for disaster recovery services receive the services in accordance with agreed-upon benchmarks and service guarantees. The procedures should ensure that customers' systems are appropriately identified, listed, prioritized, and handled in accordance with relative importance.

C. The Data Center should better publicize to its open systems customers the services it provides to them and clarify the roles

and responsibilities that it and its customers play in disaster recovery efforts. This information should be included in contracts for services and provided in summary form to the appropriately responsible individual at the customer organization.

Data Center Does Not Have Sufficient Process for Identifying High-Risk Assets

Proper identification of critical IT assets helps ensure those assets are properly protected. It also helps organizations define priorities for its systems and applications for disaster recovery purposes. The Data Center, however, has not yet performed the work necessary to formally identify its high-risk assets.

Identification of high-risk assets is necessary–According to the International Organization for Standardization and the International Electrotechnical Commission, organization-critical or high-risk assets could be informational, such as databases, system documentation, user manuals, and business continuity plans; software assets, such as application software and development tools; or physical assets, such as computer equipment, communications equipment, and removable media.

According to the Information Systems and Audit Control Association's Control Objectives for Information and Related Technologies, organizations typically possess a wide range of IT resources and infrastructure, such as applications, information, hardware, operating systems, database management systems, networks, multimedia, and facilities. Some of these resources are more important and play a more critical role in the organization's operations than others. For example, organizations will often use a network firewall to permit or deny network transmissions based on a set of established rules. If this feature were inoperative, then the network would be susceptible to various threats, such as unauthorized access. According to IT standards and best practices, an organization should maintain an inventory of critical network devices, services, information, and applications; and should assign corresponding security risk ratings to these assets. Additionally, identifying high-risk assets is a necessary step in order to allow an organization to define priorities for all of its systems and applications as part of its disaster recovery framework.

Data Center has not yet formally identified all of its critical assets–The Department possesses a range of IT assets with varying degrees of importance and criticality, which it uses to perform and

support its business functions. However, the Data Center has not performed the work necessary to formally identify all of its critical IT assets or to document the importance and level of protection appropriate for those assets. Although the Data Center maintains an inventory of all active assets, such as hardware, software, and printers, as required by state policy promulgated by the Arizona Strategic Enterprise Technology Division, this inventory does not contain all the elements necessary to ensure a complete IT inventory. For example, it is missing information on network configuration, services, and Internet Protocol (IP) addresses, and does not identify the criticality and business value of the assets it contains.[7]

Proper identification of critical IT assets helps ensure those assets are properly protected. It also helps the organization direct the proper amount of resources toward protecting those assets and not waste time and effort protecting assets that are not critical. It is also essential to an organization in performing its business continuity planning activities.

Recommendation 1.2

The Data Center should establish, implement, and maintain a formal inventory and a documented process for identifying and categorizing its organization-critical and high-risk assets. The IT inventory should contain information on applications, data, hardware, software, network resources and services, and facilities; and should assign corresponding security risk ratings to these assets.

Lack of Well-Established Data Classification Program Could Affect Ability to Prevent Unauthorized Access, Modification, Disclosure, or Destruction of Sensitive Data

The purpose of data classification is to provide a framework for classifying and protecting information resources. It also helps organizations better manage data compliance requirements and risks and helps to ensure that the proper amount of resources are expended to protect the data an organization uses and maintains. Although the Data Center began developing a data classification program in 2007, the Department has not yet actually initiated the process of identifying, inventorying, or classifying data.

[7] IP addresses are numerical labels assigned to each device on a computer network that uses Internet Protocol for communication. An IP address identifies a resource on a network and helps to route traffic between that resource and other resources.

Data classification involves categorizing information by level of sensitivity and helps organizations identify proper protections to put in place–Data classification is the process of categorizing information to show its level of sensitivity and the degree of protection needed when handling the information. A data classification process helps organizations categorize the information they use and maintain so that they can effectively identify the types of data that are available, where that data is located, what level of access protections are needed for the data, and whether the protections they implement meet business, statutory, or regulatory compliance requirements.

The need and manner required to protect information varies depending on a number of factors, including the sensitivity of the data, the availability of the data from other sources, and the length of time for which the data is relevant and viable. Data classification also helps organizations better manage data compliance requirements and risks; and helps to ensure that the appropriate amount of resources, neither too many nor too few, are expended to protect the data it uses and maintains.

According to IT standards and best practices, an effective data classification process should protect information based on requirements such as confidentiality, be reviewed and updated regularly, and consist of an inventory of information that includes details about data ownership, a definition of appropriate security levels and protection controls, and a brief description of data retention and destruction requirements, criticality, and sensitivity.

According to state policy established by the Arizona Strategic Enterprise Technology Division, agencies should identify and classify data, communicate the classifications, segregate confidential data from public data, assign data owners to all data, and categorize and protect data and software application systems based on risk.

Department has not yet defined or implemented a data classification process–Although the Data Center began developing a data classification program in 2007, and has created some draft documents, including a data classification standard, inventory template, and questionnaire, the Department has not yet actually initiated the process of identifying, inventorying, or classifying its data. According to the Data Center, shortages in department resources resulting in a reduction in employees and a lengthy policy approval process have prevented the Department from establishing and implementing a formal data classification process. The Data Center indicated that it needs to have full review and approval from the legal team and then approval from all of the Department's assistant directors in order to get a policy or

standard published. According to the Data Center, the data classification policy, which was sent to management in March 2011, has received approval from the Department's legal team after 2 months of review, and as of December 2011 had been reviewed by the State Privacy Officer, as requested by the State Chief Information Officer. It is currently being amended as warranted and the Department is working on scheduling a final review with the privacy group. It would then be sent again to the legal counsel prior to publishing the standard.

Lack of a data classification system puts the Department at risk of not meeting statutory and regulatory requirements–Without an effective data classification system, the Department could be at risk of not meeting statutory requirements and the resulting failure to adequately protect sensitive information could result in financial liability and civil penalties. For instance, Arizona Revised Statutes (A.R.S) §41-4172 indicates that all governmental agencies "shall develop and establish commercially reasonable procedures to ensure that entity identifying information or personal identifying information that is collected or obtained by the governmental agency is secure and cannot be accessed, viewed or acquired unless authorized by law." In addition, A.R.S. §44-7501 requires any person or entity in Arizona holding computerized records to notify individuals about compromised personal information if the compromise places these individuals at risk of substantial economic loss. The statute also establishes civil penalties for failure to notify without unreasonable delay persons whose information was compromised.

Additionally, the Department has statutory obligations with regard to any criminal history information records it houses. The Department cannot disseminate these records nor can it confirm or deny the existence of such a record.[8] In addition, these records need to be protected against unauthorized access, disclosure, or modification.

Recommendation 1.3

To help ensure that sensitive data is properly protected, the Department should:

A. Complete its development, review, and implementation of a documented organization-wide data classification policy and process.

B. Ensure that its process is based on risks and requirements, such as confidentiality and sensitivity of the information, consisting of an inventory of information

[8] A.R.S. §41-1750 (Q)(3)(4).

classification details that includes assigned classification, identity of the information owner, and a brief description of information classified; and that it is communicated to all affected parties, reviewed, and updated regularly.

CHAPTER 2: SECURITY ISSUES

According to the National Institute of Standards and Technology, a successful IT security program consists of: 1) developing IT security policy that reflects business needs tempered by known risks; 2) informing users of their IT security responsibilities, as documented in agency security policy and procedures; and 3) establishing processes for monitoring and reviewing the program. A security management process is needed to maintain the integrity of information and protect IT resources. This process should include establishing and maintaining IT security roles and responsibilities, policies, standards, and procedures; performing security monitoring and periodic testing; and implementing corrective actions for identified security weaknesses or incidents. An effective security management process protects all IT assets and minimizes the business impact of security vulnerabilities and incidents.

Auditors reviewed several of the Data Center's areas of responsibility that are normally part of an IT security program. Specifically, auditors addressed risk assessment, security compliance, computer security awareness training, network security, incident response management, and logging and monitoring of systems, and found that the Department is lacking in each of these critical areas. Auditors found that policies are either missing or insufficient; security awareness training is inadequate; and regular monitoring is not being performed. Specifically:

- The Data Center does not have any formal procedures for how to conduct risk assessments and has not performed any since at least 2006. As a result, the Department may not be able to adequately protect sensitive information or critical IT infrastructure by avoiding or reducing security threats or identifying and implementing controls needed to protect its systems against such threats,
- The Data Center does not have a formal policy, comprehensive process, or effective enforcement mechanism for security compliance; as a result, many of the Data Center's IT-related policies are not being consistently followed or communicated.
- The Department's security awareness training policy is insufficient, does not meet state security awareness program requirements, and is not being consistently followed.
- The Data Center does not effectively use all of the IT security control mechanisms and tools at its disposal to further limit access to its IT resources and to identify and mitigate vulnerabilities that may exist with those resources.
- Some of the Data Center's policies and standards for incident response are only in draft form, there is a lack of

coordination and understanding between the units involved in incident response, and there is no overall oversight of incident management.

- The Data Center does not regularly monitor most security-related logs nor does it have any formalized procedures to provide guidance on what events to look for or how often reviews should be done.

Lack of Risk Assessment Process Could Hinder Ability to Protect Sensitive Information or Critical Infrastructure

Risk assessments help to identify potential threats within an organization and to determine the controls needed to reduce the risk associated with them. The Data Center, however, does not have processes or procedures for risk assessments and does not perform any on a proactive basis.

Risk assessments help identify potential threats and guide action needed–Risk assessments are used to identify potential threats within an organization, such as unexpected loss of, unauthorized access to, or potential disruption of information resources; and to determine the controls needed to reduce the risk associated with those threats. A detailed risk assessment process should assign responsibility; mandate regular assessments; create an inventory of IT assets, including hardware, software, and data; contain a structured methodology for assessing risks; document results and potential impact of results; use results to make changes to the organization's security program; and report results to top management.

Data Center has no procedures for risk assessments and has not performed one since at least 2006–Although department policy indicates that risk assessments should be performed annually or when significant changes are made to information resources, the Department does not have any documented procedures on how risk assessments should be conducted. The Data Center could not produce any documentation of risk assessments it has performed and auditors were unable to identify a process the Data Center uses for performing risk assessments. The Data Center's information security manager indicated that it does not perform any proactive risk assessments but said they would be done on an as-needed basis. Despite that, he indicated none have been done since 2006, when he joined the Department.

Recommendation 2.1

The Department should establish and implement a process for performing risk assessments that assigns responsibility, mandates

regular assessments, contains a structured methodology for assessing risks, documents results and potential impact of results, uses results to make changes to the organization's security program, and reports results to top management. Additionally, the Department should perform risk assessments on an annual schedule or as significant changes are made to information resources as outlined in its current policy.

Data Center Does Not Have Effective Process or Enforcement Mechanism for Communicating About and Ensuring Security Compliance

Security compliance efforts help ensure that security policies are being followed and are effective. The Data Center, however, does not have processes or procedures detailing how to evaluate, enforce, or monitor compliance, and its efforts in this area are limited.

Security compliance processes help ensure effectiveness of security efforts–A well-designed security compliance process enables an organization to ensure that existing policies, procedures, and standards related to security are communicated, enforced, and effective in keeping the organization compliant with its business requirements. According to IT standards and best practices, an effective compliance process consists of obtaining regular confirmation of compliance with established security policies from process owners, ensuring that internal and external compliance reviews are performed against those policies, and implementing a process to monitor and report on noncompliance issues.

Data Center lacks processes to effectively monitor compliance with security requirements–The Data Center has an Information Security Policy that includes requirements for many security-related areas defined by IT standards and best practices, such as an information security committee, risk assessments, data classification, and physical security controls; however, it does not have processes or written procedures that provide guidance and details on how to evaluate, monitor, or enforce compliance with these requirements. Additionally, although the Department performs some limited compliance activities, such as reviews of the physical security of its data center and network vulnerability scans for some department servers, no comprehensive compliance process exists. In addition, auditors found that IT-related policies and procedures that exist are not consistently being followed. For instance:

- Auditors reviewed the Information Security Policy, which

indicates that an information security committee should be organized to regularly assess and review the effectiveness, impact, and appropriateness of the Department's security policies and standards, with input from business units on security-related issues. However, auditors found that the Department does not have a formal committee organized and the ad hoc committee it has does not include representation from key functional areas, does not meet regularly, and has no process to prioritize security initiatives as required by its policy.[9]

- The Data Center's Information Security Policy indicates that its Information Security Manager is responsible for reviewing and updating the policy annually. However, this policy was made effective in April 2007 and has not been reviewed or updated since then.

- Although the Data Center has another policy, the Access Control Policy, that states user accounts should be locked from further use following three unsuccessful login attempts and applies to all of the Department's internal applications, auditors found that one such application used by the Help Desk did not have this control in place. According to the individual responsible for that area, he had no knowledge that the Data Center's policy existed or that he was required to follow it.

According to the Data Center, it has not had adequate staffing in the compliance area to develop written procedures and perform compliance reviews.

Recommendation 2.2

The Department should establish and implement a formal security compliance process, which consists of obtaining regular confirmation of compliance from process owners, ensuring that internal and external compliance reviews are performed against internal policies, and implementing a process to monitor and report on noncompliance issues. As a component of its compliance process, the Department should include an enforcement mechanism to ensure that policies are effective and are being followed.

[9] Key functional areas as described in the Information Systems Audit and Control Association's "Control Objectives for Information and Related Technologies" include internal audit, human resources, operations, IT security, and legal.

Computer Security Awareness Training Policies and Requirements Not Being Met

Security awareness education is critical to help ensure that information security problems and incidents are detected and prevented. The Department's policy related to security awareness training is insufficient, does not meet state security awareness program requirements, and is not being consistently followed.

Security awareness training critical to efforts to help detect and prevent security problems–Security awareness education is a critical component of an organization's efforts to help detect and prevent information security problems and incidents. As a result, the Arizona Strategic Enterprise Technology Division created a state-wide standard to define criteria for a security training and awareness program at each agency. The standard is designed to educate state employees about their requirements to protect state information and IT resources, and to provide the knowledge and skills necessary to fulfill IT security responsibilities for the State. The standard defines the content of a security awareness training program. It also indicates that agencies should clearly define and document key personnel IT security and roles, and make the training commensurate with the level of access and expertise required in relation to the system and information resources for which the employee is responsible. Further, the state-wide standard says that all state employees should receive security training when they are hired, prior to being provided any access to state IT systems and resources, and should have their security awareness training updated annually or upon occurrence of a specific event, such as a change in job responsibilities or employment status.

The standard defines the minimum requirements for the content of an agency's security awareness training material. For example, it says such materials should:

- include information about the employee's personal responsibility for IT security and the importance of complying with all state-wide and agency security policies and standards;
- include or reference the state-wide policy for IT security, state-wide security standards, and state-wide policies for e-mail and Internet use;
- enable staff to identify and evaluate threats, vulnerabilities, and risks specific to the agency's data and IT resources;
- enable staff to better understand social engineering persuasion techniques that may be used to deceive them into revealing confidential, private, or privileged information

that could compromise agency data and IT resources;
- include technical alternatives, methods, and standards that represent best practices appropriate to agency information and IT resources that can be utilized to effectively implement safeguards; and
- cover other topics such as:
    - staff's responsibility to report IT-security-related issues;
    - legal requirements for data;
    - privacy expectations;
    - the agency's password requirements;
    - incident response procedures;
    - agency acceptable use policies for e-mail and Internet use;
    - encryption technologies and the transmission of sensitive/confidential information over the Internet; and
    - physical security.

The standard also indicates that agencies should regularly review and update the training material it uses; make it available to staff; and incorporate formal evaluation and feedback mechanisms to gauge the appropriateness and effectiveness of its security awareness and training programs, techniques, and materials.

Department's security awareness training policy is insufficient, does not meet state program requirements, and is not being consistently followed–Although the Department's policy related to security awareness training has a requirement that assigns responsibility to its Business Units to ensure all persons using ADOA information resources complete required security awareness and acceptable use of ADOA information resources training prior to authorizing access to ADOA information resources, and annually thereafter, it does not define what that training should entail or include other requirements spelled out in the state policy. For example, it does not include requirements for specialized training based upon job role; updated training when an employee changes jobs; regular review of the effectiveness of its training efforts, including formal evaluation and feedback mechanisms; and coverage of other specific elements, such as social engineering, encryption technologies, and alternative methods and standards that can be used to implement safeguards.

In addition, in lieu of receiving actual training or specifically designed security awareness training material, a majority of department employees are asked to sign, and then annually reconfirm, their acknowledgement of an acceptable use of information resources standard. This standard, however, does not provide coverage of security awareness program elements

required by state policy. For example, the acceptable use standard includes sections addressing the use of department information resources, such as using resources only for state business purposes and not connecting or installing personal devices or software to the Department's network without approval. However, it does not include any information on securing passwords and data, physical security of workstations, identifying potential security risks, and other components of security awareness training required by state policy. Further, auditors found that even reconfirmation of the agreements was not mandatorily required.

Auditors found that one group of department employees, those working in the Department's data center, did receive annual training on securing electronic information, which does contain some of the security awareness training elements required by state policy. Auditor review of the training found that it discusses handling sensitive information, securing access to local workstations and mobile devices, selecting strong passwords, potential scenarios in handling confidential information, and potential penalties for failing to comply with requirements. Employees who work in the Department's data center must attend this annual training, but the training is not provided to other department employees. However, this training still does not include all of the required elements outlined in state policy. For example, the training does not sufficiently address elements such the importance of complying with all State-wide and agency policies, referencing state-wide policies for e-mail and Internet use, or information about social engineering techniques

As a result of these shortcomings, the Department's employees may not be sufficiently informed about computer-related security threats and what their responsibilities are in support of the Department's security requirements, goals, and objectives.

Recommendation 2.3

A. The Department should enhance its policy related to security awareness training to include adequate guidance on what should be included in such training–and training materials–being sure to address all areas required by state policy; and should develop mechanisms to ensure that the policy is being followed by all of its Business Units.

B. As required by state policy, the Department should establish a department-wide security awareness education and training program. The program should:
    a. Be designed to ensure that employees understand relevant IT security risks and threats, the

Department's IT-related security policies, and each individual's role in carrying out those policies.
b. Incorporate a mechanism to periodically evaluate the program's effectiveness and make changes to it as necessary.
c. Consider and address the type and form of training needed relevant to staff members' roles and functions.
d. Be provided annually, or upon occurrence of a specific event, such as a change in job responsibilities or employment status.

Although Steps Have Been Taken to Protect Networks and Resources, More Could Be Done to Further Limit Access and Identify and Mitigate Vulnerabilities

Network security management helps organizations ensure the protection of information in networks and supporting infrastructure. Although the Department has made efforts to protect its networks and resources, it could use tools at its disposal more effectively to identify and mitigate vulnerabilities. During security testing, auditors discovered a number of problems, including a vulnerability which allowed auditors to view sensitive information that should not have been available, such as names, social security numbers, driver's license information, birth certificates, and fingerprint images. Many of the issues found exist due to the lack of regular scanning, periodic risk assessments, and a formal configuration management policy.

Network security management necessary to protect networks– According to IT standards and best practices, the purpose of network security management is to ensure the protection of information in networks as well as that of the supporting infrastructure. Networks should be managed and controlled to protect IT assets against threats and to maintain security for systems, applications, and information contained on the network. An effective network security program employs a multi-layered approach and incorporates security devices, techniques, and related management procedures, such as firewalls and other security appliances, network segmentation and access control lists, and user account management processes. In addition, ensuring that information systems and technology are kept up-to-date can help protect them from new and evolving vulnerabilities and threats.

Department has taken many important steps but could more effectively use tools at its disposal to provide further protection– Although the Department has taken a number of important steps

to protect its computer networks and resources, auditors found that the Data Center does not effectively use all of the IT security control mechanisms and tools at its disposal to further limit access to its IT resources and to identify and mitigate vulnerabilities that may exist with those resources.

Auditors discovered a number of problems–Auditors used several tools and techniques to perform testing designed to assess the ability of unauthorized users to access the Department's networks and resources. Based on the testing performed, auditors found that many of the Department's efforts to protect its IT resources were effective at preventing unintended access from potential intruders, but more could be done. For example, the Department does not ensure that all applications use the account lockout functionality built into its access control systems.[10] Auditors identified several applications for which this feature is not enabled, including for its network user accounts; however, the feature is in place for the State's financial information system. Additionally, auditors discovered vulnerabilities in the configuration of its network and security protocols that could potentially allow unauthorized individuals to gain access to parts of its network.

Further, although the Data Center has network vulnerability identification software, it only uses the software to scan some of its IT resources and excludes a large portion of the Department's network. The Data Center explained that its current licensing agreement for the software is limited to certain segments of its network and scanning additional segments would require it to incur additional fees. In this regard the Data Center treats other department Business Units as customers and indicated that it would need to charge the other Business Units for additional scans it would perform in order to recover the additional expenses that would result. The Data Center reported that the various Business Units within the Department have declined the service due to the additional costs involved. However, failure to use the software or to perform other tests to review all department computers could result in undetected vulnerabilities within the Department's network.

In fact, when auditors performed similar scans and tests they were able to identify multiple vulnerabilities on department IT equipment that could be used to access sensitive information or disrupt department services. For example, due to a vulnerability caused by a misconfigured user account, auditors were able to access

[10] Account lockout is usually a component of a security, application, or network operating system's password policy that may be used to lock user accounts after too many failed login attempts. Once an account has been locked, the user will not be allowed to access the protected system until a pre-set time has elapsed or a network administrator has unlocked the account or reset the password.

one server and view sensitive information that should not have been available to them, such as names, social security numbers, addresses, driver's license information, birth certificates, fingerprint images, and academic transcripts.

Auditors also identified different servers with specific but commonly known vulnerabilities that could potentially allow attackers to assume authentication credentials of valid users and as a result view information or perform functions for which they are not authorized. The vulnerabilities auditors discovered could also result in valid users unknowingly being redirected to malicious Web sites, possibly increasing the risk to other department computers and its networks.

In addition, auditors found that some of the Department's servers, running specific network services, were also being used to run additional, more publicly accessible services. As a result, these servers present a higher risk to the Department's network should these servers be compromised or exploited. According to best practices, these services should be installed onto separate servers and should not be exposed to the public network, and access to them should be more restricted.

Lack of a formal configuration management policy and periodic risk assessments contribute to problems found–In addition to the lack of regular scanning to identify and then help the Department to remediate these types of issues, many of these issues exist because the Data Center does not have a formal configuration management policy, which would require that IT equipment and software be set up following a formal process with specific consideration given to security concerns. Moreover, since the Department does not perform periodic risk assessments and does not use its network vulnerability detection software to scan its entire network, the issues found by auditors persisted without being detected. A majority of vulnerabilities can be reduced or eliminated by configuring equipment and software to remove unnecessary functionality and features, and by ensuring that all servers and services have received the most recent security updates.

Recommendation 2.4

The Department should:

A. Ensure that security policies are followed and security mechanisms are in use for all applications and systems.

B. Review the configuration of its servers to ensure that only needed services are running, that services and associated user and system accounts are configured securely, and that critical services are segmented from those available through the public network.

C. Use its network vulnerability scanning software or perform other procedures to regularly test all segments of its network, identify potential vulnerabilities, and mitigate them to the extent possible.

D. Develop and implement a configuration management policy that covers its IT resources and addresses security considerations.

Weaknesses in IT Security Incident Management May Result In Inconsistent and Ineffective Incident Response

Information security incident management helps ensure that security events are monitored, detected, and responded to appropriately. Although the Data Center has some policies and standards related to incident response, they were only in draft form. In addition, there was a lack of coordination and understanding between the units involved in incident management. Specifically, auditors found the Data Center was lacking an organization-wide incident response plan or policy and did not have sufficient oversight of incident handling.

Incident management provides for well-understood and predictable responses to security events–Information security incident management involves the monitoring and detection of security events on a computer or computer network, and the execution of a well-understood and predictable response to those events. According to IT standards and best practices, incident response is a process of detecting, reporting, and responding to information security incidents, such as a breach of confidential information or an attack on a computer network. An effective incident response system should consist of a standardized, documented, organization-wide process for managing individual information security incidents. Additionally, such a process would identify roles and responsibilities and provide responding individuals with authority to make critical decisions, and would provide specific guidance on how to identify, respond to, recover from, and follow up on incidents. Similarly, state policy established by the Arizona Strategic Enterprise Technology Office requires that a written process be established for the identification, reporting, investigation, and mitigation of incidents. Further, state policy specifies that this process should address such things as

establishing an incident response team, categorizing the incident by severity, and reporting the incident to a central state-wide reporting system in a timely manner.

Data Center lacks official policies and sufficient coordination and oversight of incident response–Although the Data Center has processes in place for reporting and responding to network and computer security-related incidents, auditors found that some policies and standards for incident response were only in draft form, that there was a lack of coordination and understanding between the units involved in incident response, and that there was no overall oversight of incident management. Without adequate incident response standards and procedures in place, as well as sufficient communication between units involved in incident response, the Department cannot ensure that incidents are responded to consistently and effectively.

Auditors found that although the Data Center has some documentation and processes for responding to incidents, it did not have an organization-wide incident response plan or policy and was lacking in its oversight of incident handling. Specifically, the Department's help desk, which is the primary recipient of incident notifications, was unaware of policies and procedures used by the Data Center to identify incidents, even though, according to the Data Center, its process requires all incidents be reported to the help desk via a Remedy ticket.[11] If the incident is deemed a "security incident" it should be sent to the Data Center. However, the manager of the help desk indicated that he was not aware of the Data Center's policies for security incidents, or any other policies and procedures on incident response outside of those developed for the help desk itself. The help desk policies do not provide guidance on how to identify or report a security incident to the Data Center. Recent changes to the Department have left its plans to address incident response management uncertain. The Government Information Technology Agency (GITA), which recently merged with the Department, had its own separate incident management process. The Data Center has indicated that it has had discussions about how to combine the Data Center's incident response management functions with those that were used by GITA but that it had not yet determined how that would be done at the time of this review.

Recommendation 2.5

The Department should complete, approve, and implement an organization-wide policy and process for incident response

[11] Remedy is a software product used by the Department that provides, among other things, service and help desk and change management tracking functionality.

management. It should ensure that all the appropriate Business Units are involved and that the policies and procedures identify roles and responsibilities over incident handling, provide responding individuals with a clear plan and authority to make critical decisions, and provide information on how to identify, respond to, recover from, and follow up on incidents.

Failure to Monitor Security Logs Prevents Department from Being Able to Effectively Identify Unauthorized System Activity and Attempts to Circumvent Controls

A logging and monitoring function can assist in the early prevention and detection of unusual activities that may need to be addressed. Best practices exist to help organizations define an effective log monitoring program. Although the Data Center produces many of the logs needed, it does not regularly monitor them and has not defined a process to do so.

Events should be recorded and regular monitoring of logs should be done–IT standards and best practices indicate that important system, application, and security-related events should be recorded in logs, stored centrally, protected against unauthorized change, and analyzed on a regular basis. Logs should include relevant information such as user IDs, dates and times, key events, records of successful and rejected system access attempts, changes to system configuration, activation and de-activation of protection systems, and alarms raised by the access control system. Procedures for monitoring logs should be established and the results of monitoring activities reviewed regularly.

According to the National Institute of Standards and Technology, in its "Guide to Computer Security Log Management:"

> "A log is a record of the events occurring within an organization's systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network. Many logs within an organization contain records related to computer security. These computer security logs are generated by many sources, including security software, such as antivirus software, firewalls, and intrusion detection and prevention systems; operating systems on servers, workstations, and networking equipment; and applications.
>
> The number, volume, and variety of computer security logs have increased greatly, which has created the need for computer security log management—the process for

> generating, transmitting, storing, analyzing, and disposing of computer security log data. Log management is essential to ensuring that computer security records are stored in sufficient detail for an appropriate period of time. Routine log analysis is beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems. Logs are also useful when performing auditing and forensic analysis, supporting internal investigations, establishing baselines, and identifying operational trends and long-term problems."[12]

The National Institute of Science and Technology points out, however, that a challenge common to many organizations is balancing the limited amount of log management resources available, such as storage requirements, processing capability, and staff time needed to review logs, against a continuous supply of log data. In addition, the number of sources of log data, the inconsistent format of that data, and the need to properly secure it from loss or tampering further support the need for an effective log management process.

Best Practices Help Define Effective Log Monitoring Program Elements–According to "The Standard of Good Practice for Information Security," standards and procedures for log monitoring should include:

- Management of security event logging; for example, setting policy, defining roles and responsibilities, approving budget, and reporting;
- Identification of systems on which event logging should be enabled to help identify security-related events; for example, critical business systems, systems that have experienced a major information security incident, or systems that are subject to legislative or regulatory mandates;
- Configuration of systems to generate security-related events, including event types such as failed log-on, system crash, and deletion of user account and event attributes such as date, time, user ID, file name, IP address;
- Storage of security-related events within event logs, for example, using local systems or central servers, or by using storage provided by a third-party service provider;
- Protection of security-related event logs, for example, via encryption, access control, and backup;
- Analysis of security-related event logs, including normalization, aggregation, and correlation; and
- Retention of security-related event logs, for example, to

[12] National Institute of Standards and Technology, Special Publication 800-92, "Guide to Computer Security Log Management," September 2006.

meet legal, regulatory, and business requirements for possible forensic investigations.

Data Center Does Only Limited Monitoring of Log Data–The Department's computer systems produce many of the system, application, and network security logs needed to provide data useful in identifying attacks, fraud, errors, or other unauthorized activity; however, the Data Center does not regularly monitor most logs nor does it have any formalized procedures to provide guidance on what events to look for or how often reviews should be done. Failure to monitor security logs prevents the Department from being able to effectively identify unauthorized system activity and attempts to circumvent controls it has in place over its systems and data.

The Data Center does not have any policies and procedures for log management and does only limited monitoring of the logs it keeps. In addition, although the Data Center records and monitors some logs, it is lacking a comprehensive logging and monitoring process and staff roles and responsibilities for that function are not well defined. For instance, although the Data Center maintains that it monitors certain log files, no specific user is assigned that task on a regular basis. Additionally, the Data Center does not have any formal follow-up procedures in place for when critical events are identified. The Data Center stated that many of the log files are not monitored proactively due to workload and other issues.

Recommendation 2.6

A. The Data Center should develop and implement log management policies and procedures. Those procedures should ensure that all important system, application, and security-related events be defined and recorded in logs, stored centrally, protected against unauthorized change, and analyzed on a regular basis.

B. The Department should establish and implement formalized procedures to ensure that audit logs are regularly reviewed for critical events and that any unauthorized activity detected is investigated and addressed in a timely manner.

CHAPTER 3: IDENTITY AND USER ACCOUNT MANAGEMENT ISSUES

Identity management helps ensure that all users and their activity on IT systems are uniquely identifiable and that users' access to systems and data are in line with defined and documented business needs. Identities are enabled using authentication mechanisms, such as user accounts and passwords, and activity is controlled and monitored through both technical and procedural measures.

User account management involves the policies, processes, and procedures of managing IT user accounts and related user privileges. An effective program pertains to all types of users, including administrators and internal, external, and temporary users, and addresses activities related to requesting, approving, creating, modifying, reviewing, suspending, and closing of accounts used to access IT systems and resources.

Auditors identified deficiencies related to the Data Center's handling of generic user accounts, terminated employees' account access, and access authorization documentation. Specifically:

- The Data Center's policies and procedures for identity and user account management are not always being followed. The Department also makes use of generic user accounts, including one used for a sensitive and high-level administrative activity, and does not regularly review user accounts to ensure they are still needed and that the type of access granted is still relevant and necessary to an individual's job requirements. These weaknesses undermine accountability.
- Although the Data Center has a written policy that contains adequate guidance on removing terminated employees' access, it is not always being followed. Failure to remove accounts for terminated users in a timely manner could result in an increased risk of theft, manipulation, or misuse of sensitive or confidential information.
- Although the Data Center has a policy and an overall procedure to authorize new user account creation for systems, auditors found it is not consistently being followed. As a result it may be difficult for management to confirm that the access granted to its systems is appropriate and that the access has been properly approved for all user accounts.

Department's Use of Generic Accounts and Ineffective Policies Undermine User Control and Accountability

IT standards and best practices indicate that all user accounts should be uniquely identifiable and associated with a specific

person. They also indicate that user access lists should be reviewed on a regular basis to ensure that access is limited to required users and that the type of access provided is appropriate. While the Department has a policy that outlines the importance of these practices, it is not always being followed. Additionally, auditors identified a number of instances where accounts were being shared, including some high-level and privileged administrator accounts.

Standards and best practices provide guidance on user account management–According to IT standards and best practices, all user accounts should be uniquely identifiable and associated with a specific person. Generic accounts that are not assigned to a specific individual but instead used by multiple people thwart accountability and increase the risk of fraud and misuse.

Standards and best practices also specify that user access lists should be reviewed on a regular basis to ensure that access to systems and resources is limited to required users and that the type of access provided is appropriate. In cases where it is not practicable to link a single person to an account, such as for certain types of system accounts, additional measures, such as logging and regular monitoring and review, need to be in place to ensure that accountability is established.

Department has user account-related policy but it is not always being followed–The Department has an Access Control Policy, created by the Data Center, that reinforces the importance of these practices by requiring that all users have an individually assigned and unique user account and a secure password; however, this policy is not always being followed. Auditors found that the Department has some generic user accounts, including one used for a sensitive and high-level administrative activity. Additionally, auditors found that the Department does not regularly review user accounts to ensure they are still needed and that the type of access granted is still relevant and necessary to an individual's job requirements. These weaknesses not only undermine accountability, particularly in cases where unauthorized changes may be made, errors committed, or intentional deception or fraud occurs, but they also make it more difficult and potentially impossible to identify which user made the change or committed the error or fraud.

The Access Control Policy also says that it applies to all department employees, contractors, and other entities using department information resources. Although the policy generally contains adequate guidance on user identity and account management concerns, such as requiring regular reviews of user and administrator accounts, and ensuring access is appropriate to

the person's job duties and responsibilities, auditors noted multiple instances where users were not aware of the policy or were not sure if they were even required to follow it. For instance, employees responsible for managing access to the Arizona Financial Information System; Remedy, its help desk software package; and a security application that helps protect the Department's computers all reported that they were not aware of the access policy created by the Data Center.

Auditors found some user accounts were being shared–The need for clear user access control policies and procedures was demonstrated by the fact that auditors identified a number of instances where high-level and privileged administrator accounts were being shared among multiple people or used by individuals who did not require the level of access the accounts provided to them. Specifically, auditors found that the Department uses a number of shared or generic user accounts for some sensitive and high-level administrative activities, such as for a critical security-related application, network accounts, and a key card system that controls physical access to the Department's data center. For example, auditors found that two people had the credentials to one user account that had the ability to create, edit, and delete files that are critical to ensuring the proper functioning and operation of the security application that helps protect the confidentiality of data that resides on the Department's computers.

Further, auditors found that the Department was using a number of other generic user accounts that did not have high-level administrator access, but still had access to the Department's network data files and other resources, such as physical access to the data center itself by use of electronic key cards. According to the Data Center, these generic accounts were used at one time to provide temporary access to its systems or facilities but are no longer needed. Some of these accounts were created for use by vendors and contractors who were not certain which of their specific employees would be working at the Department. The Data Center agreed that most of the accounts auditors identified were no longer needed and it has since removed them.

Additionally, after auditors reviewed the rights associated with an application used to administer the Department's anti-virus and malware prevention software, the Data Center identified an existing user who had administrative rights to the application that was not necessary.

Recommendation 3.1

A. The Department should ensure that all of its Business Units

are adhering to the Data Center's Access Control Policy, which provides guidance on: a) ensuring all user accounts are uniquely identifiable and assigned to an individual employee; and b) periodically reviewing all user access lists to ensure that they are still needed, establish user identification, and enforce access rights appropriate to the person's job duties and responsibilities.

B. The Department should review the use of generic user accounts and should eliminate ones that are no longer needed and implement procedures to better monitor ones that are retained.

Policies on Terminated Employees Not Consistently Followed, Increasing Risk of Theft, Manipulation, or Misuse of Systems and Data

Ensuring that individuals accessing network and computer systems are properly authorized and have the access they need in line with their duties and responsibilities is a basic tenet of sound IT practices and state policy. Revoking that access when an individual terminates employment is an important control to ensure that state IT resources and data is not put at risk or improperly used or disclosed. Although the Data Center has a policy addressing requirements for terminated employees, it is not being consistently followed.

Standards and state policy dictate that access to systems be limited to individuals needing access based on job duties–IT standards and best practices, as well as state policy established by the Arizona Strategic Enterprise Technology Division, dictate that access to IT systems and resources be limited to individuals needing such access to the extent necessary to perform their required duties and responsibilities. They also state that policies and procedures should exist to ensure that unnecessary access is removed in a timely manner. Further, they indicate that management review of user access rights at regular intervals and during job changes, such as transfers, promotions, or termination of employment, is essential to help ensure that access is removed from individuals who no longer require it. Failure to remove terminated users' accounts in a timely manner could result in an increased risk of theft, manipulation, or misuse of systems and the sensitive or confidential information contained on them.

Data Center's policy not being consistently followed–Although the Data Center's Access Control Policy has a section that pertains to handling terminated employees, it is not being consistently followed. The policy contains adequate guidance on removing unneeded access, for example, requiring that accounts be kept current, that timely deletion of expired accounts occur, that action

be taken during the employee termination process, that accounts be disabled after unacceptable periods of inactivity, and that regular reviews of all user and administrator accounts occur. However, as noted, auditors found that these requirements are not being consistently met.

Auditors reviewed lists of IT user accounts that had access to the Department's network and systems and compared them against employee roster information. That analysis identified 27 instances of user accounts that were linked to terminated employees and included three terminated employees who still had accounts with access to the Department's virtual private network, which is used to remotely access the Department's systems. Further, one terminated employee still had high-level administrator access to three servers used to manage a sensitive security application. Additionally, auditors found that the access lists for most of the Department's systems are not reviewed on a periodic basis for changes and discrepancies. Accounts for users of the Arizona Financial Information System, which reside on the Department's mainframe, were an exception as those are set to automatically suspend after 30 days of inactivity and are reviewed monthly so the Department can identify and remove terminated users.

The Department was notified of these issues and took actions to remedy them during the review. According to the Department, it was relying on a product that was newly implemented to inactivate some network employee accounts based on pay status changes; however, it was not working as intended.

Recommendation 3.2

The Department should:

A. Ensure that all of its Business Units are adhering to the Access Control Policy by removing user accounts when an employee is no longer employed, and regularly reviewing access lists to identify changes needing such action.

B. Determine what problems exist with the system used to inactivate network employee accounts based on pay status and correct them, or develop alternate procedures to ensure that proper action is taken.

Inadequate Documentation Makes It Difficult to Confirm User Access Has Been Properly Authorized and Is Appropriate

IT standards, including state policy, indicate that when user accounts are created, a formal record containing all relevant information should be maintained. Although the Data Center has

made some efforts to address this requirement by establishing a policy and overall procedure to authorize new user account creation for systems, auditors found it is not consistently being followed.

Establishment of user accounts should be documented–IT standards indicate that a formal record should be maintained when user accounts are created. The record should contain evidence that the account has been authorized by an appropriate level of management and should include information about what systems, functions, and access levels the user should have. The level of access granted should be appropriate to the business purpose and consistent with the organizational security policy. Similarly, state policy indicates that system, application, and information access shall be granted via a formal and auditable procedure and should have a retrievable, associated written record of the request and subsequent authorization.

Data Center's policy not being consistently followed–Although the Data Center has a policy and an overall procedure to authorize new user account creation for systems, auditors found it is not consistently being followed. Auditors also found not all authorization forms were recorded in the ticketing system used by the help desk to manage and maintain lists of issues or support requests. The lack of adequate documentation makes it difficult for management to confirm that access granted is appropriate and has been approved for all user accounts.

The Data Center's processes require that for each new employee, the employee's manager send a "New User Request Form" to the Department's help desk requesting that an account be created and specifying the access rights the employee should have to department systems. Once received, the process requires that a ticket be created noting proper approvals. However, based on a sample of 10 of the 41 user accounts created between July 1, 2010 and May 27, 2011, auditors found almost one-third of those tested did not have the proper documentation to substantiate appropriate authorization. Although the Department uses the ticketing system to manage account creation, auditors were unable to find documentation for the accounts in question. The Department confirmed that documentation should have been available for these accounts and was unable to explain why it was not created. The Department indicated that its process is to create a ticket for every request and that the missing tickets may be the result of an oversight.

Recommendation 3.3

A. The Department should take steps to ensure that it maintains required authorization documentation on file for all new account creation requests as outlined in its policy.
B. Management should regularly conduct a review of a sample of user accounts to ensure compliance with its policy.

CHAPTER 4: CHANGE AND CONFIGURATION MANAGEMENT ISSUES

Change management refers to controlling all changes to infrastructure and applications within an organization's IT environment. Effective change management mitigates risks of negatively impacting the stability or integrity of the IT environment when changes are made.

Whereas change management focuses primarily on the handling of change requests, configuration management primarily focuses on collecting configuration information on individual components and maintaining that information in a configuration repository.

Auditors identified deficiencies related to the Data Center's handling of both change management and configuration management. Specifically:

- The Data Center lacks a formalized, documented, and approved change management process. Auditors observed that changes that are made are handled inconsistently. The weaknesses found could lead to unauthorized changes, increased risk that changes will not be applied correctly, and gaps between user expectations and business requirements that could occur and go undetected.
- The Data Center does not have a formal, defined configuration management process in place and does not maintain an inventory of configuration settings for IT resources. Failure to adequately manage configurations could result in production issues or delay the Data Center in resolving issues or restoring systems.

Data Center Lacks Formal Change Management Process

IT standards and best practices indicate that formal change management procedures should be in place to ensure satisfactory control of all changes to equipment, software, or procedures and that when changes are made, an audit log containing all relevant information should be retained. Although the Data Center has made some efforts to address change management, it does not have a formalized and coordinated change management process and lacks a set of effective policies and procedures to manage its efforts.

Change management processes help ensure changes are properly authorized, documented, and implemented–Change management would typically be composed of identification and recording of significant changes, planning and testing of changes, assessment of the potential impacts of changes, formal approval procedures for proposed changes, communication of change

details to relevant parties, and fallback procedures. The Information Systems Audit and Control Association's "Control Objectives for Information and Related Technology" states that change management policies and procedures should be documented and should include:

a. Roles and responsibilities;
b. Classification and prioritization of all changes based on business risk;
c. Assessment of impact–Assess all requests for changes in a structured way to determine the impact on the operational system and its functionality;
d. Authorization and approval of all changes by the business process owners and IT–Approvers should look at the request and specification of the change, testing of the change, and request for implementation;
e. Impact on data integrity–Assessment of change on the integrity and consistency of underlying data;
f. Emergency changes–Establish a process for defining, raising, testing, documenting, assessing, and authorizing emergency changes that do not follow the established change process;
g. Tracking, status, and reporting of changes–Establish a tracking and reporting system to document rejected changes, and communicate the status of approved, in-process, and completed changes; and
h. Change closure–Whenever changes are implemented, the associated system and user documentation and procedures should be updated accordingly.

Organizations with strong change management processes typically have a group that is given decision authority over changes made to its systems. That group, often known as a Change Advisory Board, which is typically made up of representatives of different functions within the organization, reviews proposed changes and ensures that proper analysis and authorization is done, and that changes are properly supported, before approving them.

Inadequate change management could lead to unauthorized changes and increases the risk that changes will not be applied correctly. Also, gaps between user expectations and business requirements could occur and go undetected.

Data Center does not have a coordinated change management process–Although the Data Center has made some efforts to address change management, it does not have a formalized and coordinated change management process and lacks a set of effective policies and procedures to manage its efforts. The Data Center has divided its system changes into four areas based on

the type of environment to which a change will be made: mainframe, distributed (open) systems, database, and software applications; but each is handled by a separate group within the Data Center. None of these groups have formalized, documented, and approved policies and procedures to guide them in their efforts.

The Data Center provided auditors with a draft version of a change management process document, which was first created in 2009 and most recently updated in August 2010; however, the process has not been approved and is not being used consistently by any of the groups responsible for making changes. In addition, the draft lacks clear guidance for a number of important areas related to responsibility for the process. For example, the document contains information on the role of a Change Advisory Board (board) but it does not clearly define its membership or its responsibilities or authority. Specifically, the board in use does not approve changes; instead, it functions more as a scheduling body to determine when changes will be made.

Data Center's policy is incomplete and fails to address required elements–Additionally, auditors found that the draft document is incomplete and fails to adequately address many of the elements defined by IT standards and best practices. For instance, the document does not provide adequate guidance on the need to address the classification and prioritization of changes based on business risk; the assessment of impact on the operational system and related systems; the potential impact of the change to the integrity and consistency of the underlying data or system; or the need for testing plans; or have a requirement to update system documentation upon closure and acceptance of the change.

Data Center's processes lack consistency–Auditors' review of the change management processes in use at the Data Center similarly revealed problems. Auditors found that processes used by each of the four groups responsible for making changes lack consistency, both between the groups and even within the same group for different changes. For example, auditors reviewed a sample of completed changes and found that although three of the four groups seemed to be using the Change Control Form that the Data Center had developed, the form was filled out inconsistently between the groups and was missing important elements. Specifically, the form lacks requirements for information on an impact analysis and although the form requires that a risk analysis and procedures for reverting changes back to the prior state be prepared, and that a review by programmers and others not involved with the proposed change be performed, these elements were not always documented on the change forms.

Data Center does not maintain adequate documentation of changes–Further, auditors found that the Data Center does not maintain adequate documentation of the changes made to the Department's IT systems and resources. Auditors analyzed a sample of ten changes deemed moderate to high risk and high impact for fiscal year 2011 and found that almost half were either lacking or missing documentation to support the testing, approval, or implementation of the change. [13] According to the Data Center, it was unable to provide auditors with the supporting documentation during the review because it does not consistently maintain all relevant records for each change in a central repository or location.

Enterprise Infrastructure and Communications Office has a defined change management process–One other group within the Department handles similar changes but they are outside of the Data Center's normal structure. Specifically, the group responsible for monitoring and oversight of the state-wide telecommunications contract, the Enterprise Infrastructure and Communications Office (EIC), has defined a change management process.[14] However, since it is not technically responsible for systems maintained by the Department, auditors performed only a cursory review of its processes. Auditors noted that the EIC has a more mature change management process that contains many of the items lacking in the Data Center's process and documentation. For instance, for each change, the EIC's process includes items such as risk and impact analysis, defined requirements, plans for reverting changes back to the prior state, testing plans, and a review by programmers and others not involved with the proposed change. It also had a more formalized approval process with a board that has specific authority to approve or reject changes. According to the Data Center, the EIC's change management process was established by the state-wide telecommunications contractor.

Recommendation 4.1

The Data Center should:

A. Complete development of change management policies and procedures, to include:
    a. Roles and responsibilities;
    b. Classification and prioritization of all changes based on business risk;
    c. Assessment of impact;

[13] Each change is created in the ticketing system Remedy, and within that system is a category for risk and impact. The Department stated that a user specifies the risk or impact of the change based on guidance provided in the Remedy system's user guide.

[14] The Enterprise Infrastructure and Communications (EIC) Office was formerly known as the Telecommunications Program Office (TPO).

d. Authorization and approval of all changes by the business process owners and IT;
e. Testing plans;
f. Tracking and status of changes;
g. Impact on data integrity;
h. Emergency changes;
i. Tracking, status and reporting of changes; and
j. Change closure.

B. Require the Change Control Form to be completed consistently and maintained for all changes, and to be updated to include all necessary items, such as impact analysis and testing plans.

C. Consistently maintain all relevant documentation for each change in a central repository or location.

D. Review the change control process in use by the Enterprise Infrastructure and Communications (EIC) Office and consider its applicability to the Data Center's broader IT requirements. If deemed appropriate, consider incorporation of relevant EIC practices into the Data Center's existing process.

Data Center Does Not Have a Required Formal, Defined Configuration Management Process

Configuration management in IT is used for controlling modifications to IT equipment, software, and documentation in order to protect the information system against improper modifications before, during, and after system implementation. Although required by state policy, the Data Center has not established a configuration management process.

Configuration management helps to avoid production issues and delays in system restoration–Whereas change management focuses primarily on the handling of change requests, configuration management primarily focuses on collecting information on individual components and maintaining that information in a configuration repository. IT standards and best practices indicate that an effective configuration management process should include identifying configuration items, establishing baselines, storing information in a central repository, and updating the repository as needed. Failure to adequately manage configurations could result in production issues or delay the issue resolution or system restoration.

The Arizona Strategic Enterprise Technology Division requires a

configuration management process for all state agencies, and specifies that such a process include:

1. Defined responsibilities;
2. Consistent identification of configurations of IT devices, network components, and associated software components done over the life cycle of a system, from development through testing and ultimately, operations;
3. Documented change control processes that ensure a record of all changes and updates to IT devices, operating systems, and applications software versions and releases, including when the changes were made and by whom;
4. Tracking of configuration items, including the current status, pending changes, and approved changes to configuration items; and
5. Periodic review of configurations to ensure that they are well documented and up to date.

Data Center has not yet established a configuration management process as required–Auditors found that although policies created by the Arizona Strategic Enterprise Technology Division require all state agencies to establish a configuration management process, the Data Center has not yet done so for the Department. For example, the Data Center has no formalized process for establishing baselines or updating configurations on equipment, such as firewalls or antivirus software. In addition, auditors reviewed Data Center configuration inventories and found that they did not include all required configuration information, such as software versions. Failure to adequately track and manage configurations could result in operational problems or delay the Data Center's response in resolving issues.

According to the Data Center, it has been working on implementing a configuration management process for several years, although it says it has been hampered in doing so by limited resources. The Data Center reported that the help desk ticketing system it purchased in 2006 includes a configuration management database designed to help track and manage configuration changes. It reported that in 2008 it worked with the software vendor to get the database installed and configured correctly, and that it implemented the tool in 2009. However, it says that it was not able to actually use the tool due to limited resources and it formally put the project on hold in March 2011 due to continuing limited resources and requirements to integrate the former Government Information Technology Agency into the Department.

Recommendation 4.2

The Data Center should develop and implement a documented, organization-wide configuration management process that is in-line with IT standard best practice and state requirements. The process should include defined responsibilities, consistent identification of configurations of IT devices, network components, documented change control, tracking of configuration items, and periodic review of configurations.

Policies and procedures help ensure that IT management responsibilities and obligations are met–Establishing an effective set of policies and procedures to address information technology is important to ensure that an organization's IT management responsibilities are addressed and its obligations are met. Policies and procedures also provide clear guidance to employees as to what their obligations are, and demonstrate the commitment that an organization has to addressing the management of its information technology resources. Well-documented and up-to-date policies and procedures provide staff with repeatable processes and clear expectations. Failure to clearly communicate policies and procedures could limit the accountability of staff and result in inconsistencies.

IT best practices and guidelines, and policies created by the Arizona Strategic Enterprise Technology (ASET) Division, highlight the importance of and need to establish and communicate policies and procedures over key IT areas and processes. For example, one of the ASET standards addresses the need to establish rules for appropriate use and protection of electronic data, including classifying data as either public or confidential. This helps to ensure that agencies take the proper steps and direct the appropriate amount of resources necessary to protect sensitive and critical information.

Data Center is either missing or has ineffective policies over a number of significant areas and lacks an effective enforcement mechanism–In evaluating the effectiveness of the Data Center's information security processes, auditors reviewed the Data Center's IT policies and procedures and determined that it is either missing or has ineffective policies over a number of significant IT-related areas; currently has no enforcement mechanism to ensure that the policies and procedures are followed; and has not effectively disseminated and communicated its policies and procedures throughout the Department.

Auditors found deficiencies at the Department in 12 significant IT areas, described in Table 2 on page 43. More detailed information about these deficiencies is presented in the preceding sections.

Specifically, auditors found that although the Data Center may have established an adequate policy for some of the areas reviewed, most areas were missing approved and adopted, complete, comprehensive, up-to-date, and appropriately implemented policies and procedures. In addition, in most cases auditors found that even for those areas for which the Data Center had policies in place, procedures developed to support them were ineffective in achieving the desired objective. For instance,

although these and other Data Center policies are meant to be followed on a department-wide basis, auditors determined that there is no effective monitoring or enforcement mechanism in place to ensure that happens. The Data Center has established a compliance unit that is responsible for creating, updating, and enforcing its IT-related policies and procedures, but according to the Data Center it has not had adequate staffing in the compliance area to fully meet those responsibilities.

Table 2: IT Areas with Policy Deficiencies

- Disaster Recovery–The process, policies, and procedures used to minimize the probability and impact of an IT service interruption.
- High-Risk Asset Identification–The processes for inventorying network devices, services, and applications with corresponding security risk ratings.
- Data Classification–The process for labeling information to show its level of sensitivity or the degree of protection needed when handling the information.
- Risk Assessment–The process for identifying risks such as threats and vulnerabilities, determining the probability of occurrence, the resulting impact, and the additional security controls that would lessen this impact.
- Security Compliance–The process for ensuring that existing policies, procedures, and standards related to security are enforced and effective in complying with requirements.
- Computer Security Awareness–Actions taken to regularly inform and train staff about information security risks and their responsibility to comply with policies to reduce these risks.
- Incident Response Management–The process for detecting, reporting, and responding to information security incidents, such as a breach of confidential information due to a failure of IT security safeguards or computer hacking.
- Log Management–The process for generating, transmitting, storing, analyzing, and disposing of computer security log data.
- Access Control–The process for granting or preventing access to computer systems and electronic information on a network, including the set of rules designed to enhance computer security by encouraging or requiring users to employ strong passwords and use them properly.
- Encryption Key Management–The process for protecting and storing the encryption algorithms used to secure sensitive data.
- Change Management–The process for requesting, evaluating, approving, testing, and implementing changes to IT services with minimal disruption.
- Configuration Management–The process for establishing configuration baselines for hardware and software and developing a repository where configuration settings are stored, audited, and updated as needed.

As of July 2011, the unit had no staff. The unit is authorized for three full-time employees, but two positions have remained vacant

since August 2009, due to budget constraints, and the only compliance employee resigned in May 2011.

Existing Data Center policies not always effectively disseminated or communicated within the Department–Auditors also found that even policies that the Data Center has were not being effectively disseminated or communicated to other Business Units within the Department. Moreover, although the Data Center maintains its policies on the Department's internal Web site, auditors found that key individuals responsible for IT systems and applications in other Data Centers were not aware of several of these policies. For example, as previously discussed, the Data Center has an Access Control Policy, described in Table 2 (see page 43), which outlines requirements for adding, deleting, and reviewing access to computer systems. The policy is intended to be followed for all internal systems and applications within the Department; however, auditors found that knowledge of the policy's existence outside of the Data Center was limited. Specifically, employees responsible for managing access to the Arizona Financial Information System, the State's financial accounting system, and Remedy, the Department's help desk software package, reported that they were not aware of the access policy created by the Data Center. In fact, one application owner stated that his unit followed an access control policy it had developed, although he admitted the policy had not been updated in over 15 years and had many inconsistencies with its current practices.

Recommendation 5.1

The Department should:

A. Perform a comprehensive review of its IT policies and procedures, comparing them against state-wide standards and IT best practices to 1) identify missing items, and 2) items that are incomplete, out of date, or not in use.

B. Prioritize the results from its review and develop and implement, where necessary, effective IT policies and procedures that align with business requirements and then monitor for compliance with its policies and procedures.

C. Develop a strategy that ensures that IT policies and procedures are effectively and consistently communicated and disseminated to all affected parties within the Department.

APPENDIX

Scope and Methodology

Auditors performed an initial assessment of the Data Center's efforts in the following four key IT-related areas of responsibility—the degree to which the Data Center effectively:

1) Planned and organized to develop and carry out strategy and tactics and identify ways IT can best contribute to the achievement of the Department's and State's business objectives;
2) Identified, acquired, and implemented IT solutions and integrated them into business processes;
3) Delivered required services, including management of security and continuity, service support for users, and management of data and operational facilities; and
4) Monitored and evaluated performance management, internal control, regulatory compliance, and governance.

Once the initial assessment was completed, auditors developed the following four review objectives:

- Determine if the Data Center established a data classification scheme to ensure the integrity and consistency of all data. In addition, determine if the Data Center is ensuring minimal business impact to the Department and the over 100 state agencies, boards, and commissions that rely on its equipment and systems in the event of an IT service interruption through automated solutions and by developing, maintaining, and testing IT continuity plans.
- Determine if the integrity of information and protection of IT assets is maintained through the use of a security management process. Also, determine if effective problem management is in place.
- Determine if the Data Center has efficient controls over identity management, user account management, and the exchange of sensitive data.
- Determine if the Data Center maintains an accurate, complete, and accessible collection of information on hardware and software configurations. In addition, determine if the Data Center formally managed, authorized, assessed, and controlled all changes, including emergency maintenance and patches, relating to infrastructure and applications within the production IT environment.

As a basis for the evaluation of the Data Center's IT control

environment, auditors referred to the Information Systems Audit and Control Association's Control Objectives for Information and Related Technology framework, the Arizona Strategic Enterprise Technology Division's standards, and various other IT standards and best practices. Auditors also interviewed department management and staff, reviewed documentation, and observed and tested processes related to the scope of this review.

In addition, the following methods were used in reviewing specific areas:

- To evaluate the security of the Department's systems, network, and network-related components, auditors and an independent security consultant retained by the Office of the Auditor General tested servers and network components using both automated and more detailed manual security testing techniques. Through interviews with Data Center staff and technical scanning techniques, auditors identified servers, network components, and workstations to test with automated security scans and identified potential vulnerabilities in various applications and associated servers. Additional testing was performed to allow auditors to identify the potential impact of these vulnerabilities. Because of the information's sensitive nature, specific information about the security weaknesses identified has been excluded from this report and shared only with appropriate department staff.

- To develop the Overview section, auditors compiled information about staffing and organization from department documents and conducted interviews with Data Center staff.

The Auditor General and staff express their appreciation to the Department of Administration's Information Services Data Center management and staff for their cooperation and assistance throughout the review.

DEPARTMENT RESPONSE

Janice K. Brewer
Governor

Scott A. Smith
Director

ARIZONA DEPARTMENT OF ADMINISTRATION

OFFICE OF THE DIRECTOR

100 NORTH FIFTEENTH AVENUE • SUITE 401
PHOENIX, ARIZONA 85007

(602) 542-1500

August 20, 2012

Debra K. Davenport, CPA
Auditor General
Office of the Auditor General
2910 North 44th Street, Suite 410
Phoenix, Arizona 85018

Re: Auditor General Audit of ADOA State Data Center, Draft Report dated July 24, 2012

Dear Ms. Davenport:

Thank you for the opportunity to review and comment on the Auditor General ADOA State Data Center Audit. We appreciate the professionalism and efforts of the audit team and believe that the implementation of the findings will further enhance the efficiency and effectiveness of our Agency.

Enclosed are our responses to each recommendation in the report, in the order they are listed. Our responses to your findings are generic due to the sensitivity of the security findings.

Thank you again for the opportunity to respond. Should you have any questions or would like additional information, please do not hesitate to contact me at (602) 542-1500.

Sincerely,

Scott A. Smith
Director

Enclosures

ADOA Agency Response, by Section and Finding

Auditor General Recommendations – ADOA State Data Center

Recommendation 1.1

A. The Department should:
   a. Create and formalize a comprehensive disaster recovery plan, which includes all system and infrastructure components for which it is responsible, and addresses important elements such as regulatory and contractual requirements, the Departments overall business continuity needs, IT resource management requirements and interdependencies, an analysis of business impacts, risk assessments, emergency procedures, testing and ongoing maintenance of its disaster recovery efforts.
   b. Formally document and publish the plan. The plan should include information related to the activation and notification, recovery and reconstitution phases and should include supporting documentation.
   c. Test the plan on a regular basis using realistic scenarios, as defined in the plan documented and make modifications when necessary to correct any problems identified through testing.

B. The Data Center should establish formal procedures and benchmarks to ensure that customers who contract with it for disaster recovery services receive the services in accordance with agreed-upon benchmarks and service guarantees. The procedures should ensure that customers' systems are appropriately identified, listed, prioritized and handled in accordance with relative importance.

C. The Data Center should better publicize to its open systems customers the services it provides to them and clarify the roles and responsibilities that its customers play in disaster recovery efforts. This information should be included in contracts for services and provided in summary form to the appropriately responsible individual at the customer organization.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Recommendation 1.2

The Data Center should establish, implement and maintain a formal inventory and a documented process for identifying and categorizing its organization-critical and high-risk assets. The IT inventory should contain information on applications, data, hardware, software, network resources and services, and facilities; and should assign corresponding security risk ratings to these assets.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Recommendation 1.3

To help ensure that sensitive data is properly protected, the Department should:

A. Complete its development, review and implementation of a documented organization-wide data classification policy and process.

B. Ensure that its process is based on risks and requirements such as confidentiality and sensitivity of the information, consisting of an inventory of information classification details that include assigned classification, identity of the information owner, and a brief description of information classified; and that it is communicated to all affected parties, reviewed and updated regularly.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Recommendation 2.1

The Department should establish and implement a process for performing risk assessments that assigns responsibility, mandates regular assessments, contains a structured methodology for assessing risks, documents results and potential impact of results, uses results to make changes to the organization's security program, and reports results to top management. Additionally, the Department should perform risk assessments on an annual schedule or as significant changes are made to information resources as outlined in its current policy.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Recommendation 2.2

The Department should establish and implement a formal security compliance process, which consists of obtaining regular confirmation of compliance from process owners, ensuring that internal and external compliance reviews are performed against internal policies, and implementing a process to monitor and report on non-compliance issues. As a component of its compliance process, the Department should include an enforcement mechanism to ensure that policies are effective and are being followed.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Recommendation 2.3

A. The Department should enhance its policy related to security awareness training to include adequate guidance on what should be included in such training-and training materials-being sure to address all areas required by state policy; and should develop mechanisms to ensure that the policy is being followed by all of it Business Units.

B. As required by state policy, the Department should establish a department-wide security awareness education and training program. The program should:
   a. Be designed to ensure that employees understand relevant IT security risks and threats, the Department's IT-related security policies and each individual's role in carrying out those policies.
   b. Incorporate a mechanism to periodically evaluate the programs effectiveness and make changes to it as necessary.
   c. Consider and address the type and form of training needed relevant to staff member's roles and functions.
   d. Be provided annually, or upon occurrence of a specific event, such as a change in job responsibilities or employment status.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Recommendation 2.4

The Department should:

A. Ensure that security policies are followed and security mechanisms are in use for all applications and systems.

B. Review the configuration of its servers to ensure that only needed services are running, that services and associated users and system accounts are configured securely, and that critical services are segmented from those available through the public network.

C. Use its network vulnerability scanning software or perform other procedures to regularly treat all segments of its network, identify potential vulnerabilities, and mitigate them to the extent possible.

D. Develop and implement a configuration management policy that covers its IT resources and addresses security considerations.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Recommendation 2.5

The Department should complete, approve and implement an organization-wide policy and process for incident response management. It should ensure that all the appropriate Business Units are involved and that the policies and procedures identify roles and responsibilities over incident handling, provide responding individuals with a clear incident handling, provide responding individuals with a clear plan and authority to make critical decisions, and provide information on how to identify, respond to, recover from, and follow up on incidents.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Recommendation 2.6

A. The Data Center should develop and implement log management policies and procedures. Those procedures should ensure that all important system, application and security-related events be defined and recorded in logs, stored centrally, protected against unauthorized change, and analyzed on a regular basis.

B. The Department should establish and implement formalized procedures to ensure that audit logs are regularly reviewed for critical events and that any

unauthorized activity detected is investigated and addressed in a timely manner.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Recommendation 3.1

A. The Department should ensure that all of its Business Units are adhering to the Data Center's Access Control Policy, which provides guidance on: a) ensuring all user accounts are uniquely identifiable and assigned to an individual employee; and b) periodically reviewing all user access lists to ensure that they are still needed, establish user identification, and enforce access rights appropriate to the person's job duties and responsibilities.

B. The Department should review the use of generic user accounts and should eliminate ones that are no longer needed and implement procedures to better monitor ones that are retained.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Recommendation 3.2

A. The Department should ensure that all of its Business Units are adhering to the Access Control Policy by removing user accounts when an employee is no longer employed, and regularly reviewing access lists to identify changes needing such action.

B. Determine what problems exist with the system used to inactivate network employee accounts based on pay status and correct them, or develop alternate procedures to ensure that proper action is taken.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Recommendation 3.3

A. The Department should take steps to ensure that it maintains required authorization documentation on file for all new account creation requests as outlined in its policy.

B. Management should regularly conduct a review of a sample of user accounts to ensure compliance with its policy.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Recommendation 4.1

The Data Center should:

A. Complete development of change management policies and procedures, to include:
   a. Roles and responsibilities;
   b. Classification and prioritization of all changes based on business risk;
   c. Assessment of impact;
   d. Authorization and approval of all changes by the business process owners and IT;
   e. Testing plans;
   f. Tracking and status of changes;
   g. Impact of data integrity;
   h. Emergency changes;
   i. Tracking, status and reporting of changes; and
   j. Change closure.

B. Require the Change Control Form to be completed consistently and maintained for all changes, and to be updated to include all necessary items, such as impact analysis and testing plans.

C. Consistently maintain all relevant documentation for each change in a central repository or location.

D. Review the change control process in use by the Enterprise Infrastructure and Communications (EIC) Office and consider its applicability to the Data Center's broader IT requirements. If deemed appropriate, consider incorporation of relevant EIC practices into the Data Center's existing process.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will

be implemented.

Recommendation 4.2

The Data Center should develop and implement a documented, organization-wide configuration management process that is in line with IT standard best practice and state requirements. The process should include defined responsibilities, consistent identification of configurations of IT devices, network components, documented change control, tracking of configuration items, and periodic review of configurations.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Recommendation 5.1

The Department should

A. Perform a comprehensive review of its IT policies and procedures, comparing them against state-wide standards and IT best practices to 1) identify missing items, and 2) items that are incomplete, out of date, or not in use.

B. Prioritize the results from its review and develop and implement, where necessary, effective IT policies and procedures that align with business requirements and then monitor for compliance with its policies and procedures.

C. Develop a strategy that ensures that IT policies and procedures are effectively and consistently communicated and disseminated to all affected parties within the Department.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented

INTEGRITY
ACCOUNTABILITY
MAKING A DIFFERENCE