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.

OVERVIEW

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.

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.