

# Information System Audit

## Arkansas Administrative Statewide Information System (AASIS)

### General Controls



Sen. Kevin A. Smith  
Senate Co-Chair  
Rep. Danny W. Ferguson  
House Co-Chair  
Sen. Henry "Hank" Wilkins, IV  
Senate Co-Vice Chair  
Rep. Tommy Roebuck  
House Co-Vice Chair

# Arkansas



Charles L. Robinson, CPA, CFE  
Legislative Auditor

## LEGISLATIVE JOINT AUDITING COMMITTEE DIVISION OF LEGISLATIVE AUDIT

April 12, 2002

Members of the Legislative Joint Auditing Committee:

We have performed an audit of the general controls over the Arkansas Administrative Statewide Information System (AASIS) in use from September 4, 2001 to December 1, 2001 the last day of our audit fieldwork. We conducted our audit in accordance with generally accepted governmental auditing standards.

The audit included a review and testing of controls in the following areas:

1. Operating System and Database
2. Firewall, Network Topology and Web Server
3. Management and Contingency Planning
4. Transport System and Program Change Controls

Our objectives were to test configuration, policies and procedures to obtain reasonable assurance that sufficient controls exist to: protect the application, database and web servers from unauthorized access; provide for the continuation of computer processing capabilities; ensure proper management of the AASIS computer hardware; ensure that only approved and tested system control parameters are updated to the production system; and, adequately test and approve programs before placement in the production system.

Our audit procedures consisted of designing, performing and evaluating the results of tests of these controls. We believe that our audit provides a reasonable basis for our opinion.

Because of inherent limitations of controls, errors or fraud may occur and not be detected. Also, projection of this evaluation to future periods is subject to the risk that audit procedures performed may become inadequate because of changes to these controls.

The **conclusions and recommendations** resulting from our review are contained in the attached report. We trust the information in this report will assist you in your legislative decision-making process.

DIVISION OF LEGISLATIVE AUDIT

A handwritten signature in blue ink, appearing to read "Charles L. Robinson".

Charles L. Robinson, CPA, CFE  
Legislative Auditor

April 12, 2002  
IS0000302

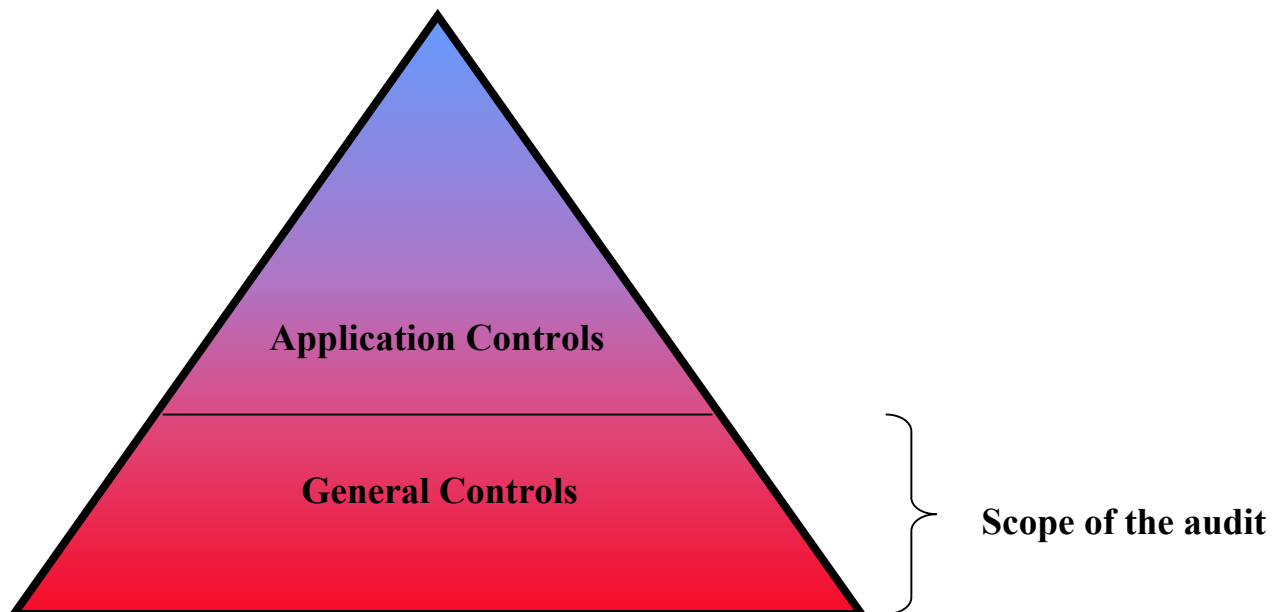
## I. OBJECTIVES

Our objectives were to test system control parameters, policies and procedures to obtain reasonable assurance that sufficient controls exist over the Arkansas Administrative Statewide Information System (AASIS) to: protect the application, database and web servers from unauthorized access; provide for the continuation of computer processing capabilities; ensure proper management of the computer hardware; ensure that only approved and tested system control parameters are updated to the production system; and, adequately test and approve programs before being placed in the production system.

## II. SCOPE AND METHODOLOGY

There are two broad categories of information systems controls: general controls and application controls. General controls comprise the processing environment including management of computer resources, file access, change control, contingency planning, backup and archiving. Application controls are specific to an application and ensure only authorized data is accepted, processing is complete and accurate, and output is reliable. Severe deficiencies in general controls could cause application controls to be ineffective because application controls are dependent on general controls. For example, a deficiency in operating system file security could cause file content application controls to be ineffective. Effective general controls form the foundation for effective application controls.

**Effective general controls form the foundation for effective application controls.**



The audit included a review and testing of controls in the following areas:

- Operating System and Database
- Firewall, Network Topology and Web Server
- Management and Contingency Planning
- Transport System and Program Change Controls

We identified the general controls in AASIS that might be relevant to the State of Arkansas' ability to record, process, summarize, and report financial data consistent with the assertions embodied in the State's financial statements. Our audit procedures consisted of designing, performing and evaluating the results of tests of these controls. We believe that our audit provides a reasonable basis for our opinion.

Because of inherent limitations of controls, errors or fraud may occur and not be detected. Also, projection of this evaluation to future periods is subject to the risk that audit procedures performed may become inadequate because of changes to these controls.

### **III. BACKGROUND**

AASIS is the new statewide accounting system purchased from the software vendor SAP Public Sector and Education, Inc. AASIS went on-line July 1, 2001 and replaces the systems formerly used by the State including the Accounting Federal Grants Management System (AFGM), Arkansas Human Resource Management System (AHRMS), and Arkansas Property Management System (APMS).

The Department of Finance and Administration was originally responsible for the implementation and management of AASIS. SAP was responsible for the design of the information technology structure supporting AASIS. In October 2001, the Governor transferred responsibility for the AASIS support center to the State's Executive Chief Information Officer. In March 2002, the Governor transferred responsibility for the AASIS support center to the Department of Information Systems (DIS). DIS and AASIS system administrators are responsible for maintaining the operating system, database, firewall, network topology, web servers, contingency planning, transport system and program change controls.

---

Management of  
AASIS is the  
responsibility of  
the Department  
of Information  
Systems.

---

#### IV. CONCLUSION

As a result of our examination and testing, numerous deficiencies in general controls were identified. These deficiencies, along with our recommendations, are listed in the remainder of this report. In our opinion, because of the severity of the deficiencies, general controls are inadequate to ensure the integrity and reliability of AASIS financial data.

---

General controls are inadequate to ensure the integrity and reliability of AASIS financial data.

---

#### V. FINDINGS AND RECOMMENDATIONS

1. A Contingency Plan includes procedures for providing hardware, software, supplies, and personnel to operate the backup computer facilities or restore the primary computer facilities in the case of a major interruption or disaster. DIS' Contingency Plan contains emergency call lists, organization charts, and procedures but does not address recovery of computer processing or backup computer facilities. This situation could cause the state to be without AASIS computer processing for an extended period of time in the event of a disaster or major interruption.

---

Contingency Plan does not address recovery of computer processing or backup computer facilities.

---

We recommend the inclusion of computer processing recovery procedures in the Contingency Plan, that arrangements be made for backup computer facilities and that the Plan be tested periodically. We further recommend that DIS management make arrangements for backup computer facilities.

#### **Management response:**

##### ***“Status:***

*DIS concurs with the above recommendations. Compliance with this recommendation depends on the establishment of a statewide business continuity policy, program funding, system design, and system implementation. **DIS looks to the legislature, the Governor’s Office, and the Office of the Executive Chief Information Officer (ECIO) for the establishment of policy & funding.***

##### ***Additional Information:***

*DIS currently has a disaster recovery plan in place that addresses the activities needed to recover from a minor outage to a large scale system outage. However, the plan has not yet*

*been fully tested. DIS is in the planning stages for a comprehensive review and implementation project for I/T Security, Disaster Recovery and Business Continuity. AASIS will be at the top of the priority list for this project.*

*When policy is developed and funds are committed, DIS will design and implement a system to allow and establish a date for a full system recovery exercise that includes equipment, data and personnel. DIS will implement a regularly scheduled system recovery exercise on an annual basis at a minimum.*

***Projected Costs to Implement:***

***AASIS: Estimate Ranges from \$240,000/yr (48 hours downtime) to \$3,900,000/yr (8 hours downtime).***

***Enterprise: Estimate Ranges from \$2,500,000 (48 hours downtime) to \$25,000,000 (limited downtime for DIS hosted critical systems- including AASIS)."***

2. Backup tapes of the AASIS system and data files are not rotated to an off-site storage location. This situation could cause financial data and AASIS system configuration to be irretrievably lost in the event of a disaster. Sound database management dictates that backups of critical system and data files should be stored at a remote site.

---

Backup tapes are not rotated to an off-site storage location.

---

We recommend that the backup copies be periodically rotated to off-site storage.

**Management response:**

***"Status:***

*DIS concurs with the above recommendation. This recommendation has been implemented.*

***Additional Information:***

*AASIS backup tapes are sent to an off site storage facility daily. DIS has provided a copy of the backup schedules and procedures that are followed for AASIS. Additionally, DIS is employing the following activities as part of its existing backup procedures:*

- a. *Review all backup schedules currently in place*
- b. *Determine that all files are being appropriately backed up*
- c. *In addition to the state offsite storage, establish a hot site location for this and other critical state applications. This is a requirement for the procurement outlined in our response to Item One*

*(1) and is dependent on when policy is defined and funds are committed.*

- d. *Using this hot site, implement online data transfers in addition to the regular tape backup process creating a fault tolerant environment. This is a requirement for the procurement outlined in our response to Item One (1) and is dependent on when policy is defined and funds are committed.”*

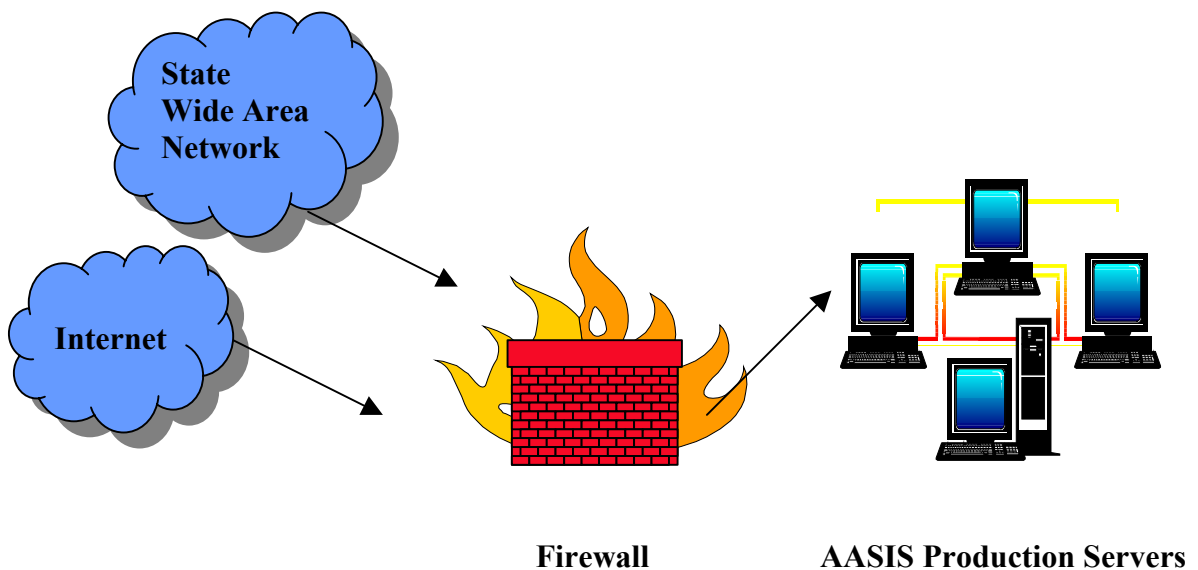
3. A firewall is a system of hardware and software components that restricts access between a network and the internet or between other networks as illustrated below.

---

The AASIS  
firewall is  
inadequate.

---

### Typical firewall setup



A firewall should:

- Allow only desired connections to pass through.
- Block other requests.
- Hide the network topology (hardware and software components) from outside networks.

The AASIS firewall is inadequate. This situation makes AASIS servers vulnerable to unauthorized access, including the server hosting AASIS financial data.

We recommend a complete firewall system be implemented that allows only necessary network traffic to communicate with AASIS servers and hides the AASIS network topology.

**Management response:**

***“Status:***

*DIS concurs with the above recommendation. Compliance with this recommendation is in progress.*

***Additional Information:***

*DIS has formulated a network three-tiered security strategy that will address this item. This is included as part of the Arkansas Secure e-Government security initiative. The state is in the process of deploying the second tier of security which will provide two levels of defense for the entire network- including AASIS. In addition to this initial implementation, DIS will be soliciting a security auditor to review the state’s enterprise network security design and confirm that the state is following security industry sound practices. After the security auditor has confirmed the state’s approach, a third tier of security will be deployed that will further protect AASIS and DIS Hosted Services.*

***Projected Costs to Implement:***

***AASIS: Addressing through DIS Hosted Services/Enterprise Security***

***Implementation Costs for Above Recommendation \$550,000***

***Enterprise: Budget Estimate \$2,650,000 (Remaining DIS Hosted Services/Enterprise Security)”***

4. One method to safeguard a networked computer against unauthorized access is to close all unneeded ports. Computers use ports with services attached to establish and maintain a communication session with another computer. AASIS servers have several ports open that are not needed for the functioning of AASIS. This situation increases the risk that an individual could gain unauthorized access to these servers by exploiting the vulnerabilities in these open ports.

We recommend that only the ports necessary for the functioning of AASIS be open.

**Management response:**

***“Status:***

*DIS concurs with the above recommendation. This recommendation has been implemented.*

***Additional Information:***

*The state has closed all ports in accordance with the SAP technical documentation. DIS has reviewed the list of open ports that are required by SAP with the Legislative Audit IT personnel.”*

5. There are numerous computer programs that have been developed to perform various functions. AASIS Financial and Human Resource personnel are responsible for testing these programs to ensure that the programs perform the functions identified in the design specification documents. However, there is no independent review (Quality Assurance Function) of the source code to determine that:
  - Source code complies with the design specifications.
  - When appropriate, source code has hard-coded “Authority-Check” to verify that the user of the programs has the authority to perform specific transactions.
  - Data tables accessed are in conformity with the intent of the program.

We recommend that AASIS management implement a quality assurance function to ensure that programs are adequately reviewed before being moved to the production system.

---

AASIS servers have several ports open that are not needed for the functioning of AASIS.

---

---

There is no independent review (Quality Assurance Function) of in-house developed programs.

---

**Management response:**

**“Status:**

*DIS concurs with the above recommendation. Full compliance with this item is in the process of being completed.*

**Additional Information:**

*The AASIS technical team has provided the Legislative Audit IT personnel with the procedures that are being followed by the AASIS technical team. In addition to this documented AASIS procedure, DIS has a Quality Plan to which AASIS deployments will be migrated. We will continue to review our procedures with Legislative Audit personnel to ensure that we are meeting our state’s requirements for the Quality Assurance Function.”*

6. Controls are inadequate to prevent or detect unauthorized modifications to the AASIS operating system. Unauthorized changes to the operating system, whether accidental or intentional, increase the risk that data and programs could be destroyed, manipulated or accessed by unauthorized individuals.

Explanations and recommendations for the above finding follow.

- There are operating system utilities, such as Trusted Computing Base, which could be used to detect penetrations and configuration changes to the operating system. These utilities store information about files, which can later be used to verify that the files have not been modified.

We recommend that these operating system utilities be used on a periodic basis to detect unauthorized changes to the operating system configuration.

- There are no formal procedures for authorizing and approving changes to the operating system. In addition there is no system in place to prevent unauthorized changes to the operating system.

We recommend implementation of change control procedures to ensure that only authorized and documented changes are made to the operating system.

---

Controls are inadequate to prevent or detect unauthorized modifications to the AASIS operating system.

---

**Management response:**

**“Status:**

*DIS concurs with the above recommendations. Full compliance with this recommendation is in the process of being completed for AASIS. Full compliance with this recommendation on all DIS hosted services depends on the establishment of a statewide policy for prevention or detection of unauthorized modifications to all operating systems, program funding, system design, and system implementation. **DIS looks to the legislature, the Governor’s Office, and the ECIO’s office for the establishment of policy & funding.***

**Additional Information:**

*In response to the first part of this recommendation, DIS is researching utilities to implement for the AASIS operating system that can detect unauthorized changes.*

*DIS does have documented procedures in place for system changes. These documented procedures have been provided to the Legislative Audit IT personnel. DIS plans to combine adherence to the documented system change procedures and the implementation of the tools to detect unauthorized changes to the AASIS operating system configuration to meet these Legislative Audit findings.*

**Projected Costs to Implement:**

**AASIS:** *These costs have not been estimated at this time.*

**Enterprise:** *These costs have not been estimated at this time.”*

7. One function of proper network management is to identify vulnerabilities in the network devices and software. Failure to identify these vulnerabilities on a timely basis could expose the network devices to unauthorized access. DIS does receive software security updates from the major vendors that support the AASIS network. However, DIS does not use network scanning software to search for vulnerabilities that could result from a missed update or improper configuration of a network device or software. Network scanning software automatically searches for vulnerabilities that could be the result of improper configuration or missed software updates.

We recommend that DIS management use network scanning software on a periodic basis to identify network vulnerabilities.

---

DIS does not use network scanning software to search for vulnerabilities.

---

## Management response:

### ***“Status:***

*DIS concurs with the above recommendation. Implementation of this recommendation has not begun at this time. Compliance with this recommendation depends on the establishment of a statewide network scanning policy, program funding, system design, and system implementation. **DIS looks to the legislature, the Governor’s Office, and the ECIO’s office for the establishment of policy & funding.***

### ***Additional Information:***

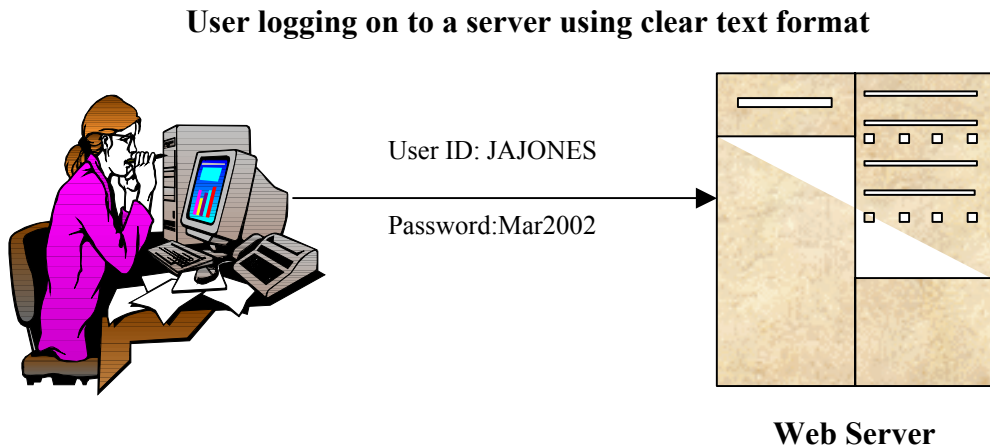
*Once the state has formulated a network security strategy that will address this item, DIS will begin working to implement this type of ongoing network analysis. This should be included as part of the Arkansas Secure e-Government security initiative. We need to fully test the deliverables, mandate that vendors train the state personnel charged with maintaining state infrastructure security, and verify that the tools are operational.*

### ***Projected Costs to Implement:***

***AASIS: These costs have not been estimated at this time.***

***Enterprise: These costs have not been estimated at this time.”***

8. Some communication methods are utilized that send a user’s ID and password over the network in clear text format as illustrated below.



This situation could allow an individual to gain knowledge of another user’s ID and password. Proper security over AASIS cannot be assured if users are able to gain knowledge of other users’ passwords.

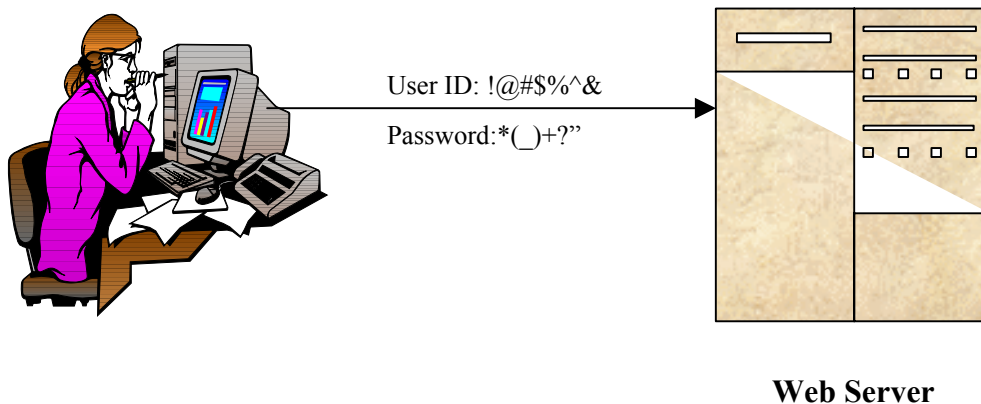
We recommend AASIS management use some form of encryption to protect passwords and other sensitive information. An example of a user logging on to a server using encryption is illustrated below.

---

Some communication methods are utilized that send a user's ID and password over the network in clear text format.

---

### User logging on to a server using encrypted format



### Management response:

#### ***“Status:***

*DIS concurs with the above recommendations. Full compliance with this recommendation is in the process of being analyzed for the best method to implement encryption. Compliance with this recommendation depends on the establishment of a statewide encryption policy, program funding, system design, and system implementation. DIS looks to the legislature, the Governor’s Office, and the ECIO’s office for the establishment of policy & funding.*

#### ***Additional Information:***

*This is an enterprise problem and should be addressed in the Arkansas’s Secure e-Government initiative. DIS is researching costs to implement an AASIS-specific solution.*

#### ***Projected Costs to Implement:***

***AASIS:*** *These costs have not been estimated at this time.*

***Enterprise:*** *These costs have not been estimated at this time.”*

9. One function of proper network management is to monitor network traffic to identify suspicious activity that might indicate an intrusion or attack on the network. There is some manual monitoring of network traffic, but AASIS does not have an automated system to identify possible intrusions. The volume of network traffic makes manual monitoring ineffective, thus increasing the risk that an intrusion or attack on AASIS could go undetected.

---

AASIS does not have an automated system to identify possible intrusions.

---

We recommend that AASIS management install an automated intrusion detection system.

**Management response:**

***“Status:***

*DIS concurs with the above recommendation. Full compliance with this recommendation is in the process of being completed.*

***Additional Information:***

*DIS is in the initial stages of implementing intrusion detection services (IDS). Full deployment across the state network of multiple IDS’ is referenced in the Arkansas Secure e-Government initiative. As part of the firewall implementation discussed in Item Three (3), an IDS will be deployed behind the firewall and in front of AASIS devices. DIS is working to build a security organization that will provide a check and balance environment between security policy and implementation of security policy across the enterprise by DIS.*

***Projected Costs to Implement:***

***AASIS: Hardware/Software Costs are included in Item 3***

***Enterprise: Hardware/Software Costs are included in Item 3***

***Preliminary additional personnel costs are estimated at 610,000 annually. This is an enterprise projection and is not based on AASIS only.”***

10. There are several active logon IDs belonging to users who are no longer AASIS contractors or employees of the State. Sound security principles dictate that only individuals currently working on AASIS have the ability to access AASIS.

---

Several active logon IDs belong to users who are no longer AASIS contractors or employees of the State.

---

We recommend that periodic reviews be performed to ensure that only authorized individuals have the ability to access AASIS.

**Management response:**

***“Status:***

*DIS concurs with the above recommendation. This recommendation has been implemented.*

***Additional Information:***

*The AASIS technical team has corrected this problem and implemented a manual process to address this issue on an ongoing basis. Also, the AASIS team has recommended the creation of an AASIS workflow which is an SAP process that will further automate this function and better utilize SAP capabilities.”*

11. The following AASIS transactions are typically reserved for system administrators:

- SM49 – allows execution of external operating system commands
- SCC4 – controls change and transport ability of configuration changes in each client
- PFCG – assigns access abilities to users (profile generator)
- STMS – enables a configuration change to be transported from one client to another
- SU01 – User account maintenance
- SU02 – User profile maintenance
- SU03 – User authorization maintenance

---

Numerous users have the ability to execute transactions that are not necessary to perform their jobs.

---

Improper use of these transactions could cause incorrect processing and permit errors in the system. Numerous users, who are not system administrators, have the ability to execute these transactions.

We recommend that users have the ability to execute only those transactions necessary to perform assigned duties.

**Management response:**

***“Status:***

*DIS concurs with the above recommendation. This recommendation has been implemented.”*

12. AASIS operating system logon and password usage controls have not been established for the following parameters.

- Minimum length of password
- Minimum number of non-alpha characters in a password
- Minimum number of alpha characters in a password
- Maximum number of weeks a password is valid
- Number of invalid login attempts before lockout
- Number of weeks before a password can be reused

---

AASIS  
operating  
system logon  
and password  
usage controls  
have not been  
established.

---

Failure to establish proper logon and password usage controls increases the likelihood that an unauthorized person could gain access to the operating system.

We recommend the establishment of logon and password controls for the above-listed parameters.

**Management response:**

***“Status:***

*DIS concurs with the above recommendation. This recommendation has been implemented.*

***Additional Information:***

*This is also addressed within the current state security architecture. Passwords must be a minimum of eight characters in length, a mixture of alpha and numeric characters, be changed at least every 90 days, not be easily determined or guessed, and not shared. This architecture has been in place since last May and AASIS now complies with this architecture in the AASIS operating system environment. Further compliance across state agencies will be verified as part of the assessment portion of the Arkansas Secure e-Government initiative.”*