

How...

ASRS Employees Deliver Service With PRIDE!

PROFESSIONALISM

We promote, strive for and expect individuals, teams, and divisions to possess professional qualities and skills to lead the organization.

- Displays a friendly, respectful and courteous demeanor even when confronted by adversity
- Has proactive and responsive approach to internal and external customer needs
- Possesses good communication and active listening skills
- Is a trusted contributor (manager, leader, SME, analyst, teammate)
- Takes personal accountability • Has subject matter expertise
- Has critical thinking skills • Has an honest, fair, non-judgmental mind-set
- Is adaptable to beneficial change • Adheres to the ASRS Code of Conduct

RESULTS

We treasure the achievements of individuals, teams, divisions and the agency that energize the organization.

- Meets goals and objectives
- Completes projects
- Produces quality work products
- Satisfies customers
- Attains individual accomplishments
- Manages risks successfully

IMPROVEMENT

We appreciate individuals, teams or divisions who drive the agency forward with new, innovative ideas and solutions.

- Promotes new ideas
- Enhances outcomes and performance
- Solves problems
- Enhances morale
- Improves relationships
- Increases efficiency, effectiveness or reduces costs

DIVERSITY

We recognize that utilizing different talents, strengths and points of view, strengthens the agency and helps propel outcomes greater than the sum of individual contributors.

- Encourages an attitude of openness and a free flow of ideas and opinions
- Treats others with dignity and respect
- Works effectively to accomplish goals with teams comprised of dissimilar individuals
- Recognizes and promotes skills in others attained on and off the job

EXCELLENCE

We celebrate individuals, teams and divisions who exceed expectations and deliver service with a PRIDE that permeates the organization.

- Surpasses member, stakeholder and associate expectations
- Demonstrates a willingness to go the extra mile to engender a positive public image
- Embraces change in a manner that inspires others
- Accepts responsibility and challenges with enthusiasm
- Takes a personal interest in promoting teamwork through effective use of communication (verbal, non-verbal, written and technological techniques)
- Creates a motivated, healthy and productive work environment that celebrates and rewards the accomplishments of others



**ARIZONA STATE
RETIREMENT SYSTEM**



ARIZONA STATE RETIREMENT SYSTEM

3300 NORTH CENTRAL AVENUE • PO BOX 33910 • PHOENIX, AZ 85067-3910 • PHONE (602) 240-2000
4400 EAST BROADWAY BOULEVARD • SUITE 200 • TUCSON, AZ 85711-3554 • PHONE (520) 239-3100
TOLL FREE OUTSIDE METRO PHOENIX AND TUCSON 1 (800) 621-3778

Paul Matson
Director

AGENDA

NOTICE OF A COMBINED PUBLIC MEETING AND POSSIBLE EXECUTIVE SESSION OF THE ARIZONA STATE RETIREMENT SYSTEM OPERATIONS AND AUDIT COMMITTEE

14th Floor Conference Room
3300 North Central Avenue
Phoenix, AZ 85012

April 12, 2016
10:30 a.m. Arizona Time

Pursuant to A.R.S. § 38-431.02, notice is hereby given to the Trustees of the Arizona State Retirement System (ASRS) Operations and Audit Committee (OAC) and to the general public that the ASRS OAC will hold a meeting open to the public on Tuesday, April 12, 2016, beginning at 10:30 a.m. Arizona Time in the 14th Floor Conference Room of the ASRS office, 3300 North Central Avenue, Phoenix, AZ 85012. Trustees of the Committee may attend either in person or by telephone conference call.

This is a regularly scheduled meeting of the OAC; however, due to possible attendance by other ASRS Board Trustees, this meeting may technically become a meeting of the Board or one of its committees. Actions taken will be consistent with OAC governance procedures. Actions requiring Board authority will be presented to the full Board for final decision.

The Chair may take public comment during any agenda item. If any member of the public wishes to speak to a particular agenda item, they should complete a request to speak form indicating the item and provide it to the Committee Administrator.

Pursuant to A.R.S. § 38-431.03(A)(3), the ASRS OAC may vote to go into executive session, which will not be open to the public, for the purpose of obtaining legal advice on any item on the Agenda.

This meeting will be teleconferenced to the ASRS Tucson office conference room at 4400 E. Broadway Boulevard, Suite 200, Tucson, Arizona 85711. The conference call to Tucson will be disconnected after 15 minutes if there are no attendees in the Tucson audience.

The Agenda for the meeting is as follows:

1. Call to Order; Roll Call; Opening Remarks.....Mr. Jeff Tyne
OAC Chair
2. Approval of the February 9, 2016, Public Meeting Minutes of the OACMr. Jeff Tyne

3. Review of Recently Conducted Audits

- City of Flagstaff – Employer Audit
- Eduprize Schools – Employer Audit
- Miami USD – Employer Audit
- North County Fire Medical District – Employer Audit
- Quartzsite Elementary School District – Employer Audit
- Ray USD – Employer Audit
- Saddle Mountain USD – Employer Audit
- Santa Cruz Valley UHSD – Employer Audit
- St. David USD – Employer Audit
- Town of Oro Valley – Employer Audit
- Tucson Airport Authority – Employer Audit

..... Mr. Anthony Guarino
Deputy Director and Chief Operations Officer
.....Mr. Bernard Glick
Chief Internal Auditor

4. Presentation, Discussion and Appropriate Action Regarding the Internal Audit Quarterly Update..

..... Mr. Anthony Guarino
.....Mr. Bernard Glick

Regarding the following agenda item, pursuant to A.R.S. § 38-431.03(A)(2), notice is hereby given to Trustees of the ASRS OAC and the general public that the ASRS OAC may vote to go into executive session, which will not be open to the public.

5. Presentation, Discussion, and Appropriate Action Regarding Issues Related to ASRS Information Technology (IT) Security Including:

- A. Presentation of the ASRS Internal IT Risk Assessment
- B. Presentation of the ASRS External IT Security Audit

..... Mr. Anthony Guarino
.....Mr. Kent Smith
Assistant Director, Technology Support Division
.....Ms. Molly Mahai
Manager, Network Information Systems
..... Mr. Thomas Keown
Information Security Officer
..... Mr. Srinivas Mukkamala
Chief Technology Officer, CAaNES

6. Requests for Future Agenda Items.....Mr. Jeff Tyne
..... Mr. Anthony Guarino

7. Call to the Public.....Mr. Jeff Tyne

Those wishing to address the ASRS Committee are required to complete a Request to Speak form before the meeting indicating their desire to speak. Request to Speak forms are available at the sign-in desk and should be given to the Committee Administrator. Trustees of the Committee are prohibited by A.R.S. § 38-431.01(G) from discussing or taking legal action on matters raised during an open call to the public unless the matters are properly noticed for discussion and legal action. As a result of public comment, the Committee Chair may direct staff

to study and/or reschedule the matter for discussion and decision at a later date.

8. Adjournment of the OAC

A copy of the agenda background material provided to the OAC Trustees (with the exception of material relating to possible executive sessions) is available for public inspection at the ASRS offices located at 3300 North Central Avenue, 14th Floor, Phoenix, Arizona and 4400 East Broadway Boulevard, Suite 200, Tucson, Arizona. The agenda is subject to revision up to 24 hours prior to meeting. These materials are also available on the ASRS website (<https://www.azasrs.gov/web/BoardCommittees.do>) approximately 48 hours prior to the meeting.

Persons(s) with disabilities may request a reasonable accommodation such as a sign language interpreter or alternate formats of this document by contacting Tracy Darmer, ADA Coordinator at (602) 240-5378 in Phoenix, at (520) 239-3100, ext. 5378 in Tucson or 1-800-621-3778, ext. 5378 outside metro Phoenix or Tucson. Requests should be made as early as possible to allow time to arrange the accommodations.

Dated April 5, 2016

ARIZONA STATE RETIREMENT SYSTEM

SIGNED COPY ON FILE

Melanie Alexander
Committee Administrator

SIGNED COPY ON FILE

Anthony Guarino
Deputy Director and Chief Operations Officer

Agenda Item #2



ARIZONA STATE RETIREMENT SYSTEM

3300 NORTH CENTRAL AVENUE • PO BOX 33910 • PHOENIX, AZ 85067-3910 • PHONE (602) 240-2000
7660 EAST BROADWAY BOULEVARD • SUITE 108 • TUCSON, AZ 85710-3776 • PHONE (520) 239-3100
TOLL FREE OUTSIDE METRO PHOENIX AND TUCSON 1 (800) 621-3778
EMAIL ADDRESS: ASKMAC@AZASRS.GOV • WEB ADDRESS: WWW.AZASRS.GOV

Paul Matson
Director

MINUTES OF A PUBLIC MEETING OF THE ARIZONA STATE RETIREMENT SYSTEM OPERATIONS AND AUDIT COMMITTEE

HELD ON
Tuesday, February 9, 2016
10:30 a.m., Arizona Time

The Operations and Audit Committee (OAC) of the Arizona State Retirement System (ASRS) met in public session in the 14th Floor Conference Room of the ASRS Office, 3300 North Central Avenue, Phoenix, Arizona 85012. Mr. Jeff Tyne, Chair, called the meeting to order at 10:30 a.m.

The meeting was teleconferenced to the ASRS office at 7660 E. Broadway, Tucson, Arizona 85710.

1. Call to Order; Roll Call; Opening Remarks

Present: Mr. Jeff Tyne, Chair
Dr. Richard Jacob
Mr. Clark Partridge (joined the meeting @ 10:35 a.m.)

A quorum of the Committee was present for the purpose of conducting business.

2. Approval of the Minutes of the December 9, 2015 Public Meeting of the OAC

Motion: Dr. Richard Jacob moved to approve the minutes of the December 9, 2015 public meeting of the OAC. Mr. Jeff Tyne seconded the motion.

By a vote of 2 in favor, 0 opposed, 0 abstentions, and 1 excused, the motion was approved.

3. Presentation, Discussion and Appropriate Action Regarding a Risk Assessment of the Contracts and Procurement Functions of the ASRS

Mr. Anthony Guarino, Deputy Director and Chief Operations Officer, introduced the topic and turned the presentation over to Ms. Lisa King, Strategic Planning Policy Analyst. Ms. King provided a brief summary of the process as the Trustees recently received an update regarding risk assessments at the January 29, 2016 Board meeting. Ms. King reiterated the ASRS bases its risk management activities on the framework recommended by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission. COSO is considered to be the industry authority on internal control, enterprise risk management and fraud deterrents. The agency believes its risk management activities have all the components in place and operating, ensuring an effective internal control environment. Ms. King added that completing risk assessments takes a considerable amount of effort and time and wanted to recognize Ms. Martha Rozen, Chief of Administrative Services, Mr. Russ Levine, Procurement and Budget Manager and their team for their efforts.

Ms. Rozen provided insight regarding the statutes and numerous guidelines that govern procurement and purchasing activities and what authority has been delegated to the agency. Ms. Rozen stated that although the ASRS does not have full autonomy, to date, the current arrangement is manageable. Ms. Rozen added the Board is kept apprised of how the ASRS is spending its money through the procurement and contract functions by way of the monthly Director's Report and annually, through the Comprehensive Annual Financial Report. Ms. Rozen turned the presentation over to Mr. Levine.

Mr. Levine provided an overview of the Enterprise Risk Management (ERM) Committee's Risk Assessment of the ASRS contracts and procurement functions. Although the ERM's conclusion is that the identified risks are manageable and that the ASRS has controls and strategies in place, for the purposes of discussion, Mr. Levine highlighted several potential risk/threats that management would like to further evaluate or reduce. ASRS staff will conduct additional industry research and analysis for services for which the ASRS contracts, cultivate a more collaborative approach to contract administration, with defined roles and responsibilities, and ensure sufficient resources are in place to achieve effective contract performance.

Throughout the presentation, Mr. Levine and Ms. Rozen responded to questions from the Committee.

Ms. King added the ERM Committee tracks future action items and conducts follow-up every six months. Updates will be presented to the Committee periodically.

4. Review of Recently Conducted Audits

Mr. Bernard Glick reviewed the following audits conducted by the Internal Audit Division (IAD).

- **City of Douglas – Employer Audit**

The IAD had four findings from the City of Douglas audit. The employer agreed with the findings and IAD's recommendations.

- **Gila Bend Unified School District – Employer Audit**

The IAD had four findings from the Gila Bend Unified School District audit. The employer agreed with the findings and IAD's recommendations.

- **Peoria Unified School District – Employer Audit**

The IAD had three findings from the Peoria Unified School District audit. The employer agreed with the findings and IAD's recommendations.

- **Sun City Fire District – Employer Audit**

The IAD had no findings from the Sun City Fire District audit.

- **ASRS Software Licensing – Internal Processes**

The IAD audit revealed the ASRS has made great progress since 2010; however, two recommendations were made by IAD. The ASRS management agreed with IAD's recommendations.

- **2015 Agency & Employer Compliance Follow-up**

The IAD presented the Committee with an employer compliance follow-up for 2015 and advised that the agency follow-up would be presented at the April 12, 2016, OAC meeting. The IAD reviewed four previously conducted audits: Town of Hayden; Altar Valley Unified

School District; Accelerated Learning Center; and Catalina Foothills Unified School District. Mr. Glick reported all findings were resolved.

5. Presentation, Discussion, and Appropriate Action Regarding the ASRS Internal Audit Peer Review Scheduled for Presentation at the June 14, 2016 OAC

Mr. Glick advised the Committee that Practice Advisory 1312 of the International Standards for the Professional Practice of Internal Auditing requires the Internal Audit Division to undergo a peer review every five years to assess whether the standards of internal audit are being met. Mr. Glick attempted to secure an organization to complete the peer review, but was unsuccessful. Mr. Glick reported that he reached out to the Vice President of the Association for Pension Plan Fund Auditors who advised him of another method to comply with the peer review requirement. Mr. Glick explained the process as follows:

- The ASRS Chief Auditor will conduct a self-assessment of the IAD following an audit program.
- Have the assessment findings independently validated.
- The individual performing the independent validation will meet with the ASRS Director and the OAC Chairman for an interview.
- Upon completion of the interviews, a report will be prepared and presented to the OAC which is currently scheduled for the June 14, 2016 meeting.

6. Presentation, Discussion and Appropriate Action Regarding the Internal Audit Quarterly Update

Mr. Bernard Glick provided a summary of the Internal Audit Quarterly Report. Mr. Glick indicated a need for a change to the Biennial Audit Plan. Due to unforeseen circumstances, two of the auditors must reduce their work hours to part-time; therefore, Mr. Glick is requesting that the Committee approve the removal of the ASRS Procurement and Bid Process audit from the 2016 and 2017 Internal Audit Biennial Work Plan. Mr. Glick explained this is the logical audit to remove because the State Procurement Office recently completed an audit in 2015.

Motion: Dr. Richard Jacob moved to accept the requested change to the Biennial Audit Plan by removing the Procurement and Bid Process audit and forward to the full ASRS Board for consideration. Mr. Clark Partridge seconded the motion.

By a vote of 3 in favor, 0 opposed, 0 abstentions, and 0 excused, the motion was approved.

7. Request for Future Agenda Items

Mr. Guarino shared a draft list, with the Committee, of future OAC topics which staff has prepared and opened up the discussion for any additional suggestions from the Committee. Dr. Jacob added he would like to see the results of the Annual Retiree Survey on a future agenda.

8. Call to the Public

There were no members of the public in Phoenix or Tucson.

9. Adjournment of the OAC

Motion: Dr. Richard Jacob moved to adjourn the meeting at 11:28 a.m. Mr. Clark Partridge seconded the motion.

By a vote of 3 in favor, 0 opposed, 0 abstentions, and 0 excused, the motion was approved.

Respectfully Submitted,

ARIZONA STATE RETIREMENT SYSTEM

Melanie Alexander
Committee Administrator

Anthony Guarino
Deputy Director and Chief Operations Officer

Agenda Item #3

City of Flagstaff Audit

**A REPORT TO THE
ARIZONA STATE RETIREMENT SYSTEM
OPERATIONS AND AUDIT COMMITTEE**

**ARIZONA STATE RETIREMENT SYSTEM
EMPLOYER AUDITS**

CITY OF FLAGSTAFF

FEBRUARY 18, 2016

The audit of the City of Flagstaff was completed February 18, 2016, for the period July 1, 2014 through June 30, 2015.

The preliminary audit objectives were to determine whether the City of Flagstaff is in compliance with Arizona Revised Statutes (A.R.S.) governing the following:

- Eligible compensation and required contributions reported to the ASRS.
- Accurate and timely enrollment of all eligible employees.
- Reporting and remitting of the employees' and employer's share of contributions.
- Medical and dental insurance premium benefits payable to retired employees.
- Retirees' return to work.

SUMMARY OF FINDING:

Based on the results of the work performed to meet the above audit objectives, the following statement summarize the finding presented to the City of Flagstaff:

- 1. City of Flagstaff did not remit ASRS contributions for seven employees who were engaged to work at least 20 hours per week for at least 20 weeks in one or more fiscal years.**

BACKGROUND

The City of Flagstaff joined the ASRS on July 1, 1956 by executing an Application and Social Security 218 Agreement. The City of Flagstaff currently has approximately 590 employees contributing to the ASRS.

DESCRIPTION OF AUDIT WORK PERFORMED

The audit work completed consisted of an examination of the employer's payroll and personnel records for the time period July 1, 2014 through July 30, 2015. The auditor reviewed pertinent documentation and interviewed the City of Flagstaff personnel from the Human Resources and Payroll departments. The auditor performed substantive tests of the employees' employment and payroll records to provide sufficient assurance that the employer is accurately reporting and remitting ASRS retirement and Long Term Disability (LTD) contributions. The following audit tests were performed:

- Review of the employer payroll records and related ASRS reports.
- Review of employees' time sheets and payroll records to determine eligibility.
- Review of the noncontributing employees' personnel and payroll records to determine compliance with the 20 hour, 20 week eligibility criteria.
- Review of the retired employees' medical and dental insurance premium benefit.
- Determine compliance with A.R.S. § 38-766.01 by reviewing the hours and weeks worked and other criteria of retired employees who returned to work.

ARIZONA STATE RETIREMENT SYSTEM
CITY OF FLAGSTAFF
FEBRUARY 18, 2016

- Determine compliance with A.R.S. § 38-766.02 requirement to pay an ACR on all retirees who have returned to work in any capacity.
- Other detailed testing as required to meet the audit objectives.

AUDITOR COMMENTS:

The City of Flagstaff personnel were cooperative, informative and helpful in providing time reports, payroll records, and other information necessary to effectively complete the ASRS audit. Audit findings and recommendations were discussed and issues resolved in a timely manner.

**A REPORT TO THE
ARIZONA STATE RETIREMENT SYSTEM
OPERATIONS AND AUDIT COMMITTEE**

**ARIZONA STATE RETIREMENT SYSTEM
EMPLOYER AUDITS**

CITY OF FLAGSTAFF

FINDINGS AND RECOMMENDATIONS

FEBRUARY 18, 2016

ARIZONA STATE RETIREMENT SYSTEM
CITY OF FLAGSTAFF
RECOMMENDATIONS

FINDING 1:

City of Flagstaff did not remit Arizona State Retirement System (ASRS) contributions for seven employees who were engaged to work at least 20 hours per week for at least 20 weeks in one or more fiscal years.

A.R.S. § 38-711, paragraph 23 defines an employee eligible to be a member in part as an employee who is “engaged to work at least twenty weeks in each fiscal year and at least twenty hours each week.” This is the basis for what is called the 20/20 eligibility criteria. A.R.S. § 38-736 states that member “contributions are required as a condition of employment and shall be made by payroll deductions. Member contributions shall begin simultaneously with membership in ASRS.”

Seven employees were engaged to work at least 20 hours per week for 20 or more weeks during the fiscal year without paying contributions when they first became eligible.

The ASRS Financial Services Department (FSD) will generate invoices for the employees’ portion of the contribution due after payment is made by the City of Flagstaff. The City of Flagstaff will be responsible to send these invoices to each employee.

The gross unreported earnings, employer and employee contributions and accrued interest due as determined by this audit are as follows:

Total Unreported Eligible Gross Earnings	<u>\$79,403</u>
Member Contributions	\$9,211
Employer Contributions	\$9,211
Estimated Interest Due	\$941
Total Estimated Due ASRS	<u>\$19,363</u>

Recommendations:

1. ASRS contributions should be withheld from all eligible earnings and employees’ earnings when an employee is engaged to work at least twenty weeks in each fiscal year and at least twenty hours per week (20/20 eligibility criteria) or when his or her status changes and he or she is reasonably expected to do so. For those employees who work irregularly from one week to the next, contributions should not be withheld until the beginning of the 20th week of working 20 or more hours.
2. The employer should have all eligible non-contributors complete online the ASRS enrollment and beneficiary forms, if applicable, so that contributions will be properly processed.

Employer Response:

The City of Flagstaff has received the draft audit finding dated February 2016 and submits the following response.

The City agrees that seven employees appear to have been engaged to work at least twenty weeks in and at least twenty hours each week in the fiscal year audit period (July 1, 2014 through June 30, 2015). The City of Flagstaff attempted to provide documentation from the hiring process to demonstrate the employees were engaged to work on a temporary basis and

ARIZONA STATE RETIREMENT SYSTEM
CITY OF FLAGSTAFF
RECOMMENDATIONS

not eligible to participate in ASRS, but were unsuccessful because the documentation was not located or included in the general six months of temporary assignment permitted per City policy. The City of Flagstaff has updated its hiring process to clearly indicate the hiring supervisor's intentions by adding a section to the vacancy request form (to fill a position) and requiring the supervisor to select one of the two options:

- This position will work less than 20 weeks at 20 hours or more; or
- This position will work more than 20 weeks at 20 hours or more.

The City has also changed the record retention process for recruitment records to ensure documentation is in order and easily reproduced.

The City of Flagstaff accepts the draft audit report recommendations. The City of Flagstaff understands it is our responsibility to notify the seven employees they are eligible for the Arizona State Retirement System benefits, assist them in enrollment and forward the employee contribution invoice upon receipt.

If you need to discuss the audit finding further, you may reach me at sanderson@flagstaffaz.gov or via phone at 928-213-2092.

Sincerely,

Signed Copy on File

Shannon Anderson
Human Resources Director
City of Flagstaff

Eduprize Schools Audit

**A REPORT TO THE
ARIZONA STATE RETIREMENT SYSTEM
OPERATIONS AND AUDIT COMMITTEE**

**ARIZONA STATE RETIREMENT SYSTEM
EMPLOYER AUDITS**

EDUPRIZE SCHOOLS

MARCH 14, 2016

ARIZONA STATE RETIREMENT SYSTEM
EDUPRIZE SCHOOLS
MARCH 14, 2016

The audit of Eduprize Schools was completed March 14, 2016, for the period July 1, 2014 through June 30, 2015.

The preliminary audit objectives were to determine whether the Eduprize Schools are in compliance with Arizona Revised Statutes (A.R.S.) governing the following:

- Eligible compensation and required contributions reported to the ASRS.
- Accurate and timely enrollment of all eligible employees.
- Reporting and remitting of the employees' and employer's share of contributions.
- Medical and dental insurance premium benefits payable to retired employees.
- Retirees' return to work.

SUMMARY OF FINDINGS:

Based on the results of the work performed to meet the above audit objectives, there were no findings presented to Eduprize Schools.

BACKGROUND

Eduprize Schools joined the ASRS on July 1, 1995 by executing an Application and Social Security 218 Agreement. Eduprize Schools currently has approximately 353 employees contributing to the ASRS.

DESCRIPTION OF AUDIT WORK PERFORMED

The audit work completed consisted of an examination of the employer's payroll and personnel records for the time period July 1, 2014 through June 30, 2015. The auditor reviewed pertinent documentation and interviewed Eduprize Schools' personnel from the Human Resources and Payroll departments. The auditor performed substantive tests of the employees' employment and payroll records to provide sufficient assurance that the employer is accurately reporting and remitting ASRS retirement and Long Term Disability (LTD) contributions. The following audit tests were performed:

- Review of the employer payroll records and related ASRS reports.
- Review of employees' time sheets and payroll records to determine eligibility.
- Review of the noncontributing employees' personnel and payroll records to determine compliance with the 20 hour, 20 week eligibility criteria.
- Review of the retired employees' medical and dental insurance premium benefit.
- Determine compliance with A.R.S. § 38-766.01 by reviewing the hours and weeks worked and other criteria of retired employees who returned to work.
- Determine compliance with A.R.S. § 38-766.02 requirement to pay an ACR on all retirees who have returned to work in any capacity.
- Other detailed testing as required to meet the audit objectives.

AUDITOR COMMENTS:

Eduprize Schools' personnel were cooperative, informative and helpful in providing FYE 2015 time reports, payroll records, and other information necessary to effectively complete the ASRS audit. Audit findings and recommendations were discussed and issues resolved in a timely manner.

Miami USD Audit

**A REPORT TO THE
ARIZONA STATE RETIREMENT SYSTEM
OPERATIONS AND AUDIT COMMITTEE**

**ARIZONA STATE RETIREMENT SYSTEM
EMPLOYER AUDITS**

MIAMI UNIFIED SCHOOL DISTRICT

FEBRUARY 2, 2016

The audit of Miami Unified School District was completed on February 2, 2016 for the period July 1, 2014 through June 30, 2015.

The preliminary audit objectives were to determine whether the Miami Unified School District is in compliance with Arizona Revised Statutes (A.R.S.) governing the following:

- Eligible compensation and required contributions reported to the ASRS.
- Accurate and timely enrollment of all eligible employees.
- Reporting and remitting of the employees' and employer's share of contributions.
- Medical and dental insurance premium benefits payable to retired employees.
- Retirees' return to work.

SUMMARY OF FINDINGS:

Based on the results of the work performed to meet the above audit objectives, the following statements summarize the findings presented to Miami Unified School District:

1. **Miami Unified School District did not remit ASRS contributions on all eligible compensation for four employees.**
2. **Miami Unified School District did not remit all of the Alternate Contribution Rate (ACR) for all its retirees who have returned to work.**
3. **Miami Unified School District did not request a refund for one member who remitted contributions on ineligible compensation.**
4. **Miami Unified School District did not ensure that all retirees returning to work complied with the requirement that they acknowledge the provisions of the statute in writing.**
5. **The Miami Unified School District did not report all demographic information for its members.**

BACKGROUND

Miami Unified School District joined the ASRS on July 1, 1957 by executing an Application and Social Security 218 Agreement. Miami Unified School District currently has approximately 150 employees contributing to the ASRS.

DESCRIPTION OF AUDIT WORK PERFORMED

The audit work completed consisted of an examination of the employer's payroll and personnel records for the time period July 1, 2014 through June 30, 2015. The auditor reviewed pertinent documentation and interviewed Miami Unified School District personnel from the Human Resources and Payroll departments. The auditor performed substantive tests of the employees'

ARIZONA STATE RETIREMENT SYSTEM
MIAMI UNIFIED SCHOOL DISTRICT
FEBRUARY 2, 2016

employment and payroll records to provide sufficient assurance that the employer is accurately reporting and remitting ASRS retirement and Long Term Disability (LTD) contributions. The following audit tests were performed:

- Review of the employer payroll records and related ASRS reports.
- Review of employees' time sheets and payroll records to determine eligibility.
- Review of the noncontributing employees' personnel and payroll records to determine compliance with the 20 hour, 20 week eligibility criteria.
- Review of the retired employees' medical and dental insurance premium benefit.
- Determine compliance with A.R.S. § 38-766.01 by reviewing the hours and weeks worked and other criteria of retired employees who returned to work.
- Determine compliance with A.R.S. § 38-766.02 requirement to pay an ACR on all retirees who have returned to work in any capacity.
- Other detailed testing as required to meet the audit objectives.

AUDITOR COMMENTS:

Miami Unified School District personnel were cooperative, informative and helpful in providing FY 2015 time reports, payroll records, and other information necessary to effectively complete the ASRS audit. Audit findings and recommendations were discussed and issues resolved in a timely manner.

**A REPORT TO THE
ARIZONA STATE RETIREMENT SYSTEM
OPERATIONS AND AUDIT COMMITTEE**

**ARIZONA STATE RETIREMENT SYSTEM
EMPLOYER AUDITS**

MIAMI UNIFIED SCHOOL DISTRICT

FINDINGS AND RECOMMENDATIONS

FEBRUARY 2, 2016

ARIZONA STATE RETIREMENT SYSTEM
MIAMI UNIFIED SCHOOL DISTRICT
RECOMMENDATIONS

FINDING 1:

Miami Unified School District did not remit Arizona State Retirement System (ASRS) contributions on all eligible compensation for four employees.

A.R.S. § 38-711(23) defines an employee eligible to be a member in part as an employee who is “engaged to work at least twenty weeks in each fiscal year and at least twenty hours each week.” This is the basis for what is called the 20/20 eligibility criteria. A.R.S. § 38-736 states that member “contributions are required as a condition of employment and shall be made by payroll deductions. Member contributions shall begin simultaneously with membership in ASRS.”

The District had 151 contributing members in the fiscal year. The District reported \$3,947,341 in eligible wages and paid \$453,153 in contributions on those wages. Four employees of the District contributed on most of their eligible compensation, but not all. Two of the members did not start reporting as soon as they became eligible. One had his final pay omitted. The last member had some payments coded so that ASRS was not withheld from those payments.

Retirement and LTD contributions will be due to the ASRS on the eligible compensation as calculated from time and pay records of the noncontributing or under-contributing employees. The ASRS Financial Services Department will generate invoices for the employees for their portion after payment is made by the District.

The gross unreported earnings, employer and employee contributions and accrued interest due as determined by this audit are as follows:

Total Unreported Eligible Gross Earnings	\$6,091
Member Contributions	707
Employer Contributions	707
Estimated Interest Due	67
Total Estimated Due ASRS	\$1,481

Recommendations:

1. The employer should notify eligible employees when there is a change in eligibility status. ASRS contributions should be withheld from employee’s earnings when an employee is engaged to work at least 20 weeks in each fiscal year and at least 20 hours per week (20/20 eligibility criteria) or when his or her status changes and he or she is reasonably expected to do so. For those employees who work irregularly from one week to the next, contributions should be withheld no later than the beginning of the twentieth week of working 20 or more hours.
2. The employer should not change employees from eligible to ineligible until the end of the fiscal year. An eligible employee generally does not become ineligible during a fiscal year.
3. The employer should remit the employer retirement contributions, LTD contributions and interest, as calculated and billed.
4. The employer should distribute to the employees the invoices that will be generated for the employees’ retirement and LTD contributions.

ARIZONA STATE RETIREMENT SYSTEM
MIAMI UNIFIED SCHOOL DISTRICT
RECOMMENDATIONS

Employer Response:

The district agrees with the finding referenced above and will make sure that all eligible employees are contributing on all positions assigned.

FINDING 2:

Miami Unified School District did not remit all of the Alternate Contribution Rate (ACR) for all its retirees who have returned to work.

A.R.S. § 38-766.02 requires that an employer “shall pay contributions at an alternate contribution rate on behalf of a retired member who returns to work in any capacity in a position ordinarily filled by an employee of the employer”. The District reported compensation and paid ACR for 18 retirees. However, one of the retirees had one pay period in fiscal year 2015 omitted. Two other eligible retirees were not reported.

The employer should have paid \$50,188 for 20 retirees, but paid \$45,328 for 18 retirees, for a compliance rate of 90%.

The ACR owed should be paid through the ASRS web site so that the exact accrued interest can be determined with the payment when it is made.

The gross eligible earnings and estimated employer ACR payments as determined by this audit are as follows:

Total Retirees’ Unreported Gross Earnings	<u>\$50,786</u>
Employer ACR Contributions	4,860
Estimated Interest Due	200
Total Estimated Due ASRS	<u>\$ 5,060</u>

Recommendations:

1. The District should pay the back ACR payments through the online system that will calculate interest owed up to the date of payment.
2. The District should pay all current and future ACR amounts owed in a timely manner.

Employer Response:

The district agrees with the finding referenced above. The district will use the ASRS system to check all employees for eligibility status.

FINDING 3:

Miami Unified School District did not request a refund for one member who remitted contributions on ineligible compensation.

A.R.S. § 38-738(A) provides for a refund of ineligible earnings. “If more than the correct amount of employer or member contributions is paid into ASRS by an employer through a mistake of

ARIZONA STATE RETIREMENT SYSTEM
MIAMI UNIFIED SCHOOL DISTRICT
RECOMMENDATIONS

fact, ASRS shall return those contributions to the employer if the employer requests return of the contributions within one year after the date of overpayments.”

The employer had 151 active members in fiscal year 2015. Only one employee was noted who had contributed in one year when not eligible to do so

The gross ineligible earnings, employer and employee pension and LTD contributions as determined by this audit are as follows:

Total Ineligible Gross Earnings	\$ 240
Ineligible Member Pension Contributions	26
Ineligible Member LTD Contributions	1
Ineligible Employer Pension Contributions	26
Ineligible Employer LTD Contributions	1
Total Estimated to be Credited to Employer	\$ 54

Recommendation:

The employer should not include ineligible compensation to ASRS. If the employer remits ineligible contributions through a mistake of fact, the employer should request a credit once the error becomes known.

Employer Response:

The district accepts the finding referenced above. It will request a credit once the error is known. The district will also verify eligibility prior to taking out contributions.

FINDING 4:

Miami Unified School District did not ensure that all retirees returning to work complied with the requirement that they acknowledge the provisions of the statute in writing.

A.R.S. § 38-766.01 provides the guidelines for retirees who wish to return to work without suspension of benefits. The A.R.S. § 38 766.01(C) states “the retired member shall acknowledge this section in writing and file the acknowledgement with the employer within thirty days of returning to work.”

ASRS requires that employers provide a copy of this acknowledgement to ASRS. A.R.S. § 38-766.02(E) states, “an employer of a retired member shall submit any reports, data, paperwork or materials that are requested by ASRS.”

At the beginning of the field work, the District had written documentation for some, but not all, of its retirees who had returned to work. Twenty retirees were working after retirement in direct employment. Ten of these did not have proper written documentation at the beginning of field work, but the District had all remaining ten retired members’ complete proper forms before the end of the field work.

ARIZONA STATE RETIREMENT SYSTEM
MIAMI UNIFIED SCHOOL DISTRICT
RECOMMENDATIONS

Recommendation:

The District should ensure that all retirees working in direct employment acknowledge in writing the conditions under which they are returning to work within 30 days of reemployment.

Employer Response:

The district accepts the finding as referenced above. We have added to the ASRS form given to all employees to include a box which states they are an ASRS retiree and will file a "Return to Work" form prior to starting work.

FINDING 5:

The Miami Unified School District did not report all demographic information for its members.

A.R.S. § 38-715 establishes the requirements to maintain the books and processing records of ASRS. A.R.S. § 38-737 says that employer contributions will be determined by the ASRS actuary every year. The actuary requires full demographic information in order to make an accurate calculation of the contribution rate.

The District reported contributions for 151 members in fiscal year 2015, most of whom had all required demographic information. At the beginning of the audit the District was informed that it had nine employees who were missing one or more of the following items of demographic information: date of birth, marital code, gender or address. The District supplied the missing information within one business day.

Recommendation:

The District should continue to ensure that all eligible members complete online enrollment prior to submitting contributions so that this information will be collected for all new employees.

Employer Response:

The district accepts the finding referenced above. All new (Eligible) employees are required to enroll themselves in the online system prior to starting work.

North County Fire Medical District Audit

**A REPORT TO THE
ARIZONA STATE RETIREMENT SYSTEM
OPERATIONS AND AUDIT COMMITTEE**

**ARIZONA STATE RETIREMENT SYSTEM
EMPLOYER AUDITS
NORTH COUNTY FIRE & MEDICAL DISTRICT
FEBRUARY17, 2016**

The audit of the North County Fire & Medical District was completed February 17, 2016 for the period July 1, 2014 through June 30, 2015.

The preliminary audit objectives were to determine whether the North County Fire and Medical District is in compliance with Arizona Revised Statutes (A.R.S.) governing the following:

- Eligible compensation and required contributions reported to the ASRS.
- Accurate and timely enrollment of all eligible employees.
- Reporting and remitting of the employees' and employer's share of contributions.
- Medical and dental insurance premium benefits payable to retired employees.
- Retirees' return to work.

SUMMARY OF FINDINGS:

Based on the results of the work performed to meet the above audit objectives, there were no findings presented to the North County Fire & Medical District.

BACKGROUND

The North County Fire & Medical District joined the ASRS on July 1, 1998 by executing an Application and Social Security 218 agreement. The North County Fire & Medical District currently has approximately 23 employees contributing to the ASRS.

DESCRIPTION OF AUDIT WORK PERFORMED

The audit work completed consisted of an examination of the employer's payroll and personnel records for the time period July 1, 2014 through June 30, 2015. The auditor reviewed pertinent documentation and interviewed the North County Fire & Medical District personnel from the Human Resources and Payroll departments. The auditor performed substantive tests of the employees' employment and payroll records to provide sufficient assurance that the employer is accurately reporting and remitting ASRS retirement and Long Term Disability (LTD) contributions. The following audit tests were performed:

- Review of the employer payroll records and related ASRS reports.
- Review of employees' time sheets and payroll records to determine eligibility.
- Review of the noncontributing employees' personnel and payroll records to determine compliance with the 20 hour, 20 week eligibility criteria.
- Review of the retired employees' medical and dental insurance premium benefit.
- Determine compliance with A.R.S. § 38-766.01 by reviewing the hours and weeks worked and other criteria of retired employees who returned to work.
- Determine compliance with A.R.S. § 38-766.02 requirement to pay an ACR on all retirees who have returned to work in any capacity.
- Other detailed testing as required to meet the audit objectives.

AUDITOR COMMENTS:

The North County Fire & Medical District personnel were cooperative, informative and helpful in providing time reports, payroll records, and other information necessary to effectively complete the ASRS audit.

Quartzsite
Elementary School
District Audit

**A REPORT TO THE
ARIZONA STATE RETIREMENT SYSTEM
OPERATIONS AND AUDIT COMMITTEE**

**ARIZONA STATE RETIREMENT SYSTEM
EMPLOYER AUDITS**

QUARTZSITE ELEMENTARY SCHOOL DISTRICT

MARCH 29, 2016

The audit of Quartzsite Elementary School District (District) was completed on March 29, 2016 for the period July 1, 2014 through June 30, 2015.

The preliminary audit objectives were to determine whether the District is in compliance with Arizona Revised Statutes (A.R.S.) governing the following:

- Eligible compensation and required contributions reported to the ASRS.
- Accurate and timely enrollment of all eligible employees.
- Reporting and remitting of the employees' and employer's share of contributions.
- Medical and dental insurance premium benefits payable to retired employees.
- Retirees' return to work.

SUMMARY OF FINDINGS:

Based on the results of the work performed to meet the above audit objectives, there were no findings presented to the District.

BACKGROUND

The District joined the ASRS on July 1, 1986 by executing an Application and Social Security 218 Agreement. The District currently has approximately 45 employees contributing to the ASRS.

DESCRIPTION OF AUDIT WORK PERFORMED

The audit work completed consisted of an examination of the employer's payroll and personnel records for the time period July 1, 2014 to June 30, 2015. The auditor reviewed pertinent documentation and interviewed District personnel from the Human Resources and Payroll departments. The auditor performed substantive tests of the employees' employment and payroll records to provide sufficient assurance that the employer is accurately reporting and remitting ASRS retirement and Long Term Disability (LTD) contributions. The following audit tests were performed:

- Review of the employer payroll records and related ASRS reports.
- Review of employees' time and payroll records to determine eligibility.
- Review of the noncontributing employees' personnel and payroll records to determine compliance with the 20 hour, 20 week eligibility criteria.
- Review of the retired employees' medical and dental insurance premium benefit.
- Determine compliance with A.R.S. § 38-766.01 by reviewing the hours and weeks worked and other criteria of retired employees who returned to work.
- Determine compliance with A.R.S. § 38-766.02 requirement to pay an ACR on all retirees who have returned to work in any capacity in a position ordinarily filled by an employee.
- Other detailed testing as required to meet the audit objectives.

AUDITOR COMMENTS:

The District personnel were cooperative, informative and helpful in providing FY 2015 time reports, payroll records, and other information necessary to effectively complete the ASRS audit.

Ray USD Audit

**A REPORT TO THE
ARIZONA STATE RETIREMENT SYSTEM
OPERATIONS AND AUDIT COMMITTEE**

**ARIZONA STATE RETIREMENT SYSTEM
EMPLOYER AUDITS**

RAY UNIFIED SCHOOL DISTRICT

FEBRUARY 22, 2016

The audit of Ray Unified School District was completed February 22, 2016 for the period July 1, 2014 through June 30, 2015.

The preliminary audit objectives were to determine whether the Ray Unified School District is in compliance with Arizona Revised Statutes (A.R.S.) governing the following:

- Eligible compensation and required contributions reported to the ASRS.
- Accurate and timely enrollment of all eligible employees.
- Reporting and remitting of the employees' and employer's share of contributions.
- Medical and dental insurance premium benefits payable to retired employees.
- Retirees' return to work.

SUMMARY OF FINDINGS:

Based on the results of the work performed to meet the above audit objectives, the following statements summarize the findings presented to Ray Unified School District:

- 1. Ray Unified School District did not remit the alternate contribution due on all eligible wages for four of its returned to work retirees.**
- 2. Ray Unified School District did not request a credit for three ineligible members who remitted contributions for part of a fiscal year.**

BACKGROUND

Ray Unified School District joined the ASRS on July 1, 1966 by executing an Application and Social Security 218 Agreement. Ray Unified School District currently has approximately 80 employees contributing to the ASRS.

DESCRIPTION OF AUDIT WORK PERFORMED

The audit work completed consisted of an examination of the employer's payroll and personnel records for the time period July 1, 2014 through June 30, 2015. The auditor reviewed pertinent documentation and interviewed Ray Unified School District personnel from the Human Resources and Payroll departments. The auditor performed substantive tests of the employees' employment and payroll records to provide sufficient assurance that the employer is accurately reporting and remitting ASRS retirement and Long Term Disability (LTD) contributions. The following audit tests were performed:

- Review of the employer payroll records and related ASRS reports.
- Review of employees' time sheets and payroll records to determine eligibility.
- Review of the noncontributing employees' personnel and payroll records to determine compliance with the 20 hour, 20 week eligibility criteria.
- Review of the retired employees' medical and dental insurance premium benefit.

ARIZONA STATE RETIREMENT SYSTEM
RAY UNIFIED SCHOOL DISTRICT
FEBRUARY 22, 2016

- Determine compliance with A.R.S. § 38-766.01 by reviewing the hours and weeks worked and other criteria of retired employees who returned to work.
- Determine compliance with A.R.S. § 38-766.02 requirement to pay an ACR on all retirees who have returned to work in any capacity.
- Other detailed testing as required to meet the audit objectives.

AUDITOR COMMENTS:

Ray Unified School District personnel were cooperative, informative and helpful in providing FYE 2015 time reports, payroll records, and other information necessary to effectively complete the ASRS audit. Audit findings and recommendations were discussed and issues resolved in a timely manner.

**A REPORT TO THE
ARIZONA STATE RETIREMENT SYSTEM
OPERATIONS AND AUDIT COMMITTEE**

**ARIZONA STATE RETIREMENT SYSTEM
EMPLOYER AUDITS**

RAY UNIFIED SCHOOL DISTRICT

FINDINGS AND RECOMMENDATIONS

FEBRUARY 22, 2016

ARIZONA STATE RETIREMENT SYSTEM
RAY UNIFIED SCHOOL DISTRICT
RECOMMENDATIONS

FINDING 1:

Ray Unified School District (USD) did not remit the alternate contribution due on all eligible wages for four of its returned to work retirees.

A.R.S. § 38-766.02 provides the guidelines for payment of the alternate contribution rate (ACR) for retirees who work after retirement. According to the statute, “an employer shall pay contributions at an alternate contribution rate on behalf of a retired member who returns to work in any capacity in a position ordinarily filled by an employee.” The ACR is to be “applied to the compensation, gross salary or contract fee of a retired member who meets the requirements of this section.”

Ray USD had four return to work retiree’s where no alternate contribution was remitted on all eligible wages.

The estimated alternate contribution due, excluding interest, as determined by this audit is as follows:

Total Gross Earnings	<u>\$13,630</u>
Total Estimated Alternate Contribution Due	<u>\$1,304</u>

Recommendation:

Ray USD should contact its contributions accounting representative at the Arizona State Retirement System (ASRS) to make arrangements for payment, including interest, of the alternate contribution due.

Employer Response:

Ray USD will make it a standard practice to check the eligibility of all new employees through the ASRS website. Ray USD will contact ASRS to make payment arrangements for the amount the District owes.

FINDING 2:

Ray USD did not request a credit for three ineligible members who remitted contributions for part of a fiscal year.

A.R.S. § 38-738(A) provides for a return of ineligible earnings. “If more than the correct amount of employer or member contributions is paid into ASRS by an employer through a mistake of fact, ASRS shall return those contributions to the employer if the employer requests return of the contributions within one year after the date of overpayments.”

The gross ineligible earnings and employer and employee contributions to be credited to the employer’s account, as determined by this audit are as follows:

Total Gross Earnings	<u>\$12,731</u>
Member Contributions	1,469
Employer Contributions	1,469
Total Credit Due	<u>\$2,938</u>

ARIZONA STATE RETIREMENT SYSTEM
RAY UNIFIED SCHOOL DISTRICT
RECOMMENDATIONS

Recommendations:

1. Ray USD should contact its contributions accounting representative at the ASRS to make arrangements to take this available credit.
2. The employer should notify each eligible employee/retiree when there is a change in eligibility status. ASRS contributions should not be withheld from part-time employees' earnings when an employee is not engaged to work at least 20 weeks in each fiscal year and at least 20 hours per week (20/20 membership criteria). For those employees who work irregularly from one week to the next, contributions should not be withheld until the beginning of the twentieth week of working 20 or more hours.
3. The employer should not adjust the amount it owes to the ASRS by reducing it by the amount owed by the ASRS because the accounts are separate.

Employer Response:

Ray USD will carefully monitor employees to see if they are engaged in the 20/20 membership criteria. Ray USD will contact ASRS for reimbursement of overpayment.

Saddle Mountain USD Audit

**A REPORT TO THE
ARIZONA STATE RETIREMENT SYSTEM
OPERATIONS AND AUDIT COMMITTEE**

**ARIZONA STATE RETIREMENT SYSTEM
EMPLOYER AUDITS
SADDLE MOUNTAIN UNIFIED SCHOOL DISTRICT
MARCH 3, 2016**

The audit of Saddle Mountain Unified School District was completed on March 3, 2016 for the period July 1, 2014 through June 30, 2015.

The preliminary audit objectives were to determine whether the Saddle Mountain Unified School District is in compliance with Arizona Revised Statutes (A.R.S.) governing the following:

- Eligible compensation and required contributions reported to the ASRS.
- Accurate and timely enrollment of all eligible employees.
- Reporting and remitting of the employees' and employer's share of contributions.
- Medical and dental insurance premium benefits payable to retired employees.
- Retirees' return to work.

SUMMARY OF FINDINGS:

Based on the results of the work performed to meet the above audit objectives, the following statements summarize the findings presented to Saddle Mountain Unified School District:

- 1. Saddle Mountain Unified School District did not:**
 - Remit ASRS contributions for two employees who were engaged to work at least 20 hours per week for at least 20 weeks in a fiscal year.
 - Remit ASRS contributions on all eligible compensation for three employees.
- 2. Saddle Mountain Unified School District did not remit all of the Alternate Contribution Rate (ACR) for its retirees who have returned to work.**
- 3. Saddle Mountain Unified School District remitted contributions on ineligible compensation for three employees.**
- 4. Saddle Mountain Unified School District did not ensure that all retirees working after retirement complied with the requirement that they acknowledged in writing the conditions under which they were returning to work.**
- 5. The Saddle Mountain Unified School District did not report all demographic information for its members.**

BACKGROUND

Saddle Mountain Unified School District joined the ASRS on July 1, 1967 by executing an Application and Social Security 218 Agreement. Saddle Mountain Unified School District currently has approximately 160 employees contributing to the ASRS.

DESCRIPTION OF AUDIT WORK PERFORMED

The audit work completed consisted of an examination of the employer's payroll and personnel records for the time period July 1, 2014 to June 30, 2015. The auditor reviewed pertinent documentation and interviewed Saddle Mountain Unified School District personnel from the Human Resources and Payroll departments. The auditor performed substantive tests of the employees' employment and payroll records to provide sufficient assurance that the employer is accurately reporting and remitting ASRS retirement and Long Term Disability (LTD) contributions. The following audit tests were performed:

- Review of the employer payroll records and related ASRS reports.
- Review of employees' time and payroll records to determine eligibility.
- Review of the noncontributing employees' personnel and payroll records to determine compliance with the 20 hour, 20 week eligibility criteria.
- Review of the retired employees' medical and dental insurance premium benefit.
- Determine compliance with A.R.S. § 38-766.01 by reviewing the hours and weeks worked and other criteria of retired employees who returned to work.
- Determine compliance with A.R.S. § 38-766.02 requirement to pay an ACR on all retirees who have returned to work in any capacity in a position ordinarily filled by an employee.
- Other detailed testing as required to meet the audit objectives.

AUDITOR COMMENTS:

Saddle Mountain Unified School District personnel were cooperative, informative and helpful in providing FY 2015 time reports, payroll records, and other information necessary to effectively complete the ASRS audit. Audit findings and recommendations were discussed and issues resolved in a timely manner.

**A REPORT TO THE
ARIZONA STATE RETIREMENT SYSTEM
OPERATIONS AND AUDIT COMMITTEE**

**ARIZONA STATE RETIREMENT SYSTEM
EMPLOYER AUDITS
SADDLE MOUNTAIN UNIFIED SCHOOL DISTRICT
FINDINGS AND RECOMMENDATIONS**

MARCH 3, 2016

ARIZONA STATE RETIREMENT SYSTEM
SADDLE MOUNTAIN UNIFIED SCHOOL DISTRICT
RECOMMENDATIONS

FINDING 1:

Saddle Mountain Unified School District did not:

- **Remit ASRS contributions for two employees who were engaged to work at least 20 hours per week for at least 20 weeks in a fiscal year.**
- **Remit ASRS contributions on all eligible compensation for three employees.**

A.R.S. § 38-711(23) defines an employee eligible to be a member in part as an employee who is “engaged to work at least twenty weeks in each fiscal year and at least twenty hours each week.” This is the basis for what is called the 20/20 eligibility criteria. A.R.S. § 38-736 states that member “contributions are required as a condition of employment and shall be made by payroll deductions. Member contributions shall begin simultaneously with membership in ASRS.”

The District reported contributions for 162 members in fiscal year 2015. The District remitted \$633,045 in contributions on \$5,515,360 of eligible compensation. Two employees of the District worked at least 20 hours per week for 20 or more weeks during the fiscal year without paying contributions when they first became eligible and through the end of the fiscal year. These employees should have been participating in the ASRS when they were engaged to work these hours, and no later than the period when they actually reached the twentieth week of working 20 or more hours.

Three employees did not contribute on all eligible compensation. For each of these members, the start of contributions was delayed.

Retirement and LTD contributions will be due to the ASRS on the eligible compensation as calculated from time and pay records of the noncontributing or under-contributing employees. The ASRS Financial Services Department will generate invoices for the employees for their portion after payment is made by the District.

The gross unreported earnings, employer and employee contributions and accrued interest due as determined by this audit are as follows:

Total Unreported Eligible Gross Earnings	\$19,303
Member Contributions	2,239
Employer Contributions	2,239
Estimated Interest Due	242
Total Estimated Due ASRS	\$4,720

Recommendations:

1. The employer should notify each eligible employee when there is a change in eligibility status. ASRS contributions should be withheld from an employee’s earnings when an employee is engaged to work at least 20 weeks in each fiscal year and at least 20 hours per week (20/20 eligibility criteria) or when his or her status changes and he or she is reasonably expected to do so. For those employees who work irregularly from one week to the next, contributions should be withheld no later than the beginning of the twentieth week of working 20 or more hours.

ARIZONA STATE RETIREMENT SYSTEM
SADDLE MOUNTAIN UNIFIED SCHOOL DISTRICT
RECOMMENDATIONS

2. The employer should have all eligible noncontributing employees' complete ASRS online enrollment and beneficiary forms, if applicable, so that contributions will be properly processed.
3. The employer should not change employees from eligible to ineligible until the end of the fiscal year. An eligible employee generally does not become ineligible during a fiscal year.
4. The employer should remit the employer retirement contributions, LTD contributions and interest, as calculated and billed.
5. The employer should distribute to the employees the invoices that will be generated for the employees' retirement and LTD contributions.

Employer Response:

The district will notify each eligible employee(s) when there is a change in eligibility status. ASRS contributions will be withheld from employee's earnings when an employee has worked at least 20 weeks and at least 20 hours per week (20/20 eligibility criteria) in a fiscal year, contributions will be withheld no later than the beginning of the twentieth week of working 20 hours or more.

When applicable the district will have all eligible noncontributing employees complete ASRS online enrollment and beneficiary forms. The district will not change employee status from eligible to ineligible until the end of the fiscal year.

The district will remit the employer retirement contributions, LTD contributions and interest as calculated and billed. The district will make every effort to distribute to the employees the invoices that will be generated for the employee's retirement and LTD contributions.

FINDING 2:

Saddle Mountain Unified School District did not remit all of the Alternate Contribution Rate (ACR) for its retirees who have returned to work.

A.R.S. § 38-766.02 requires that an employer "shall pay contributions at an alternate contribution rate on behalf of a retired member who returns to work in any capacity in a position ordinarily filled by an employee of the employer". The District reported compensation and paid ACR for 10 retirees. However, three other retirees were not reported. One of these was an independent contractor. The employer was unaware that independent contractors were also subject to the ACR. The District paid \$46,036 of the total \$62,889 owed, which is a 73% compliance rate of payment.

The ACR should be paid through the ASRS web site so that the exact accrued interest can be determined with the payment when it is made.

The gross eligible earnings and estimated employer ACR payments as determined by this audit are as follows:

ARIZONA STATE RETIREMENT SYSTEM
SADDLE MOUNTAIN UNIFIED SCHOOL DISTRICT
RECOMMENDATIONS

Total Retirees' Unreported Gross Earnings	<u>\$179,195</u>
Employer ACR Contributions	<u>16,853</u>
Estimated Interest Due	<u>1,300</u>
Total Estimated Due ASRS	<u>\$ 18,153</u>

Recommendations:

1. The District should pay the back ACR payments through the online system that will calculate interest owed up to the date of payment.
2. The District should pay all current and future ACR amounts owed in a timely manner.

Employer Response:

The district will work with ASRS to pay the back ACR payments through the online system, including interest owed up to the date of payment.

The district will pay all current and future ACR amounts owed in a timely manner.

FINDING 3:

Saddle Mountain Unified School District remitted contributions on ineligible compensation for three employees.

A.R.S. § 38-711(23) defines an employee eligible to be a member in part as an employee who is "engaged to work at least twenty weeks in each fiscal year and at least twenty hours each week." This is the basis for what is called the 20/20 eligibility criteria. The employees identified in the audit did not meet the 20/20 eligibility criteria and therefore were not eligible to participate in ASRS.

A.R.S. § 38-738(A) provides for a refund of ineligible earnings. "If more than the correct amount of employer or member contributions is paid into ASRS by an employer through a mistake of fact, ASRS shall return those contributions to the employer if the employer requests return of the contributions within one year after the date of overpayments."

The gross ineligible earnings, employer and employee pension and LTD contributions as determined by this audit are as follows:

Total Ineligible Gross Earnings	<u>\$4,236</u>
Ineligible Member Pension Contributions	<u>486</u>
Ineligible Member LTD Contributions	<u>5</u>
Ineligible Employer Pension Contributions	<u>486</u>
Ineligible Employer LTD Contributions	<u>5</u>
Total Estimated to be Credited to Employer	<u>\$ 982</u>

Recommendations:

1. The employer should request a credit for these ineligible payments.

ARIZONA STATE RETIREMENT SYSTEM
SADDLE MOUNTAIN UNIFIED SCHOOL DISTRICT
RECOMMENDATIONS

2. The employer should review its records to see if any of these or other employees contributed on ineligible compensation in the current year, a year not covered by the audit, and request a credit for those ineligible amounts.
3. The employer may want to review its available records to identify any other ineligible payments in years not covered by the audit.

Employer Response:

The district has requested a credit for the ineligible payments. The district will review our records to determine if these or any other employees contributed on ineligible compensation in the current year, not covered by the audit, and request a credit for the ineligible amounts. The district may review its available records to identify any other ineligible payments in years not covered by the audit.

FINDING 4:

Saddle Mountain Unified School District did not ensure that all retirees working after retirement complied with the requirement that they acknowledge in writing the conditions under which they were returning to work.

A.R.S. § 38-766.01 provides the guidelines for retirees who wish to return to work without suspension of benefits. The A.R.S. § 38-766.01(C) states “the retired member shall acknowledge this section in writing and file the acknowledgement with the employer within thirty days of returning to work.”

ASRS requires that employers provide a copy of this acknowledgement ASRS. A.R.S. § 38-766.02(E) states, “an employer of a retired member shall submit any reports, data, paperwork or materials that are requested by ASRS.”

At the beginning of field work, the District had written documentation for some, but not all, of its retirees who had returned to work. Twelve retirees were working after retirement in direct employment. Seven of these did not have proper written documentation at the beginning of field work, and the District did not have any of these retired members complete proper forms before the end of field work.

Recommendation:

The District should ensure that all retirees working in direct employment complete the online return to work form, within 30 days of reemployment, to acknowledge in writing the conditions under which they are returning to work.

Employer Response:

The district will ensure that all known retirees working in direct employment complete the online return to work form, within 30 days of reemployment, to acknowledge in writing the conditions under which they are returning to work.

ARIZONA STATE RETIREMENT SYSTEM
SADDLE MOUNTAIN UNIFIED SCHOOL DISTRICT
RECOMMENDATIONS

FINDING 5:

The Saddle Mountain Unified School District did not report all demographic information for its members.

A.R.S. § 38-715 establishes the requirements to maintain the books and processing records of ASRS. A.R.S. § 38-737 says that employer contributions will be determined by the ASRS actuary every year. The actuary requires full demographic information in order to make an accurate calculation of the contribution rate.

The District reported contributions for 162 members in fiscal year 2015, most of whom had all required demographic information. At the beginning of the audit the District was informed that it had 9 employees who were missing one or more of the following items of demographic information: date of birth, marital code, gender or address. The District supplied the missing information within a week.

Recommendation:

The District should continue to ensure that all eligible members complete online enrollment prior to submitting contributions so that this information will be collected for all new employees.

Employer Response:

The district will continue to ensure all eligible members complete online enrollment prior to submitting contributions.

Santa Cruz Valley UHSD Audit

**A REPORT TO THE
ARIZONA STATE RETIREMENT SYSTEM
OPERATIONS AND AUDIT COMMITTEE**

**ARIZONA STATE RETIREMENT SYSTEM
EMPLOYER AUDITS
SANTA CRUZ VALLEY UNION HIGH SCHOOL DISTRICT
FEBRUARY 25, 2016**

The audit of Santa Cruz Valley Union High School District was completed on February 25, 2016 for the period July 1, 2014 through June 30, 2015.

The preliminary audit objectives were to determine whether the Santa Cruz Valley Union High School District is in compliance with Arizona Revised Statutes (A.R.S.) governing the following:

- Eligible compensation and required contributions reported to the ASRS.
- Accurate and timely enrollment of all eligible employees.
- Reporting and remitting of the employees' and employer's share of contributions.
- Medical and dental insurance premium benefits payable to retired employees.
- Retirees' return to work.

SUMMARY OF FINDINGS:

Based on the results of the work performed to meet the above audit objectives, the following statements summarize the findings presented to Santa Cruz Valley Union High School District:

- 1. Santa Cruz Valley Union High School District did not request a refund for seven employees who remitted contributions even though they were working less than 20/20 at this employer.**
- 2. Santa Cruz Valley Union High School District reported pay dates as pay period end dates, which made the determination of the reporting date off by nine days.**
- 3. Santa Cruz Valley Union High School District did not ensure that all retirees returning to work under A.R.S. §§ 38-766.01 and 38-766.02 complied with the requirement that they acknowledge the provisions of the statute in writing.**
- 4. The Santa Cruz Valley Union High School District did not report all demographic information for its members.**

BACKGROUND

Santa Cruz Valley Union High School District joined the ASRS on January 1, 1955 by executing an Application and Social Security 218 Agreement. Santa Cruz Valley Union High School District currently has approximately 55 employees contributing to the ASRS.

DESCRIPTION OF AUDIT WORK PERFORMED

The audit work completed consisted of an examination of the employer's payroll and personnel records for the time period July 1, 2014 through June 30, 2015. The auditor reviewed pertinent documentation and interviewed Santa Cruz Valley Union High School District personnel from the Human Resources and Payroll departments. The auditor performed substantive tests of the employees' employment and payroll records to provide sufficient assurance that the employer is accurately reporting and remitting ASRS retirement and Long Term Disability (LTD) contributions. The following audit tests were performed:

ARIZONA STATE RETIREMENT SYSTEM
SANTA CRUZ VALLEY UNION HIGH SCHOOL DISTRICT
FEBRUARY 25, 2016

- Review of the employer payroll records and related ASRS reports.
- Review of employees' time sheets and payroll records to determine eligibility.
- Review of the noncontributing employees' personnel and payroll records to determine compliance with the 20 hour, 20 week eligibility criteria.
- Review of the retired employees' medical and dental insurance premium benefit.
- Determine compliance with A.R.S. § 38-766.01 by reviewing the hours and weeks worked and other criteria of retired employees who returned to work.
- Determine compliance with A.R.S. § 38-766.02 requirement to pay an ACR on all retirees who have returned to work in any capacity.
- Other detailed testing as required to meet the audit objectives.

AUDITOR COMMENTS:

Santa Cruz Valley Union High School District personnel were cooperative, informative and helpful in providing FY 2015 time reports, payroll records, and other information necessary to effectively complete the ASRS audit. Audit findings and recommendations were discussed and issues resolved in a timely manner.

**A REPORT TO THE
ARIZONA STATE RETIREMENT SYSTEM
OPERATIONS AND AUDIT COMMITTEE**

**ARIZONA STATE RETIREMENT SYSTEM
EMPLOYER AUDITS**

SANTA CRUZ VALLEY UNION HIGH SCHOOL DISTRICT

FINDINGS AND RECOMMENDATIONS

FEBRUARY 25, 2016

ARIZONA STATE RETIREMENT SYSTEM
SANTA CRUZ VALLEY UNION HIGH SCHOOL DISTRICT
RECOMMENDATIONS

FINDING 1:

Santa Cruz Valley Union High School District did not request a refund for seven employees who remitted contributions even though they were working less than 20/20 at this employer.

A.R.S. § 38-738(A) provides for a refund of ineligible earnings. "If more than the correct amount of employer or member contributions is paid into the ASRS by an employer through a mistake of fact, the ASRS shall return those contributions to the employer if the employer requests return of the contributions within one year after the date of overpayments."

The employer had 57 active members in fiscal year 2015. Seven of those were contributing even though they were working less than 20 weeks of at least 20 hours in the fiscal year. The members used to be eligible under the dual employment statutes. They could have remained eligible under certain grandfathering provisions, but these members had a break in service at the secondary employment of 30 days or more and lost that eligibility.

The gross ineligible earnings, employer and employee pension and LTD contributions as determined by this audit are as follows:

Total Ineligible Gross Earnings	<u>\$20,166</u>
Ineligible Member Pension Contributions	2,132
Ineligible Member LTD Contributions	48
Ineligible Employer Pension Contributions	2,132
Ineligible Employer LTD Contributions	48
Total Estimated to be Credited to Employer	<u>\$ 4,360</u>

Recommendations:

1. The employer should request a credit for these ineligible amounts.
2. The employer should return the employees' share directly to the employees.
3. In the future, the employer should not include compensation for any employee who has not been engaged to work 20/20 in a fiscal year. All members who have lost their grandfathering status can no longer reclaim it.

Employer Response:

The District will be requesting a credit for the seven employees identified in the ASRS Audit with our next payroll. Going forward, the District will request a credit for ineligible amounts if the District discovers any errors in payroll. The District will also ensure the Payroll Clerk receives proper training by attending the mandated annual ASRS trainings in the fall.

FINDING 2:

Santa Cruz Valley Union High School District reported pay dates as pay period end dates, which made the determination of the reporting date off by nine days.

A.R.S. § 38-736(B) states that the "employer shall pay the member contributions required of members on account of compensation earned." It is not to be reported on the basis of when it

ARIZONA STATE RETIREMENT SYSTEM
SANTA CRUZ VALLEY UNION HIGH SCHOOL DISTRICT
RECOMMENDATIONS

was paid, but when it was earned. This reporting requirement helps to ensure that members receive proper service credit for months in which they work. In addition, interest is charged to employers who delay payments of contributions, so delaying the reporting date gives the employer additional days to report and make payment without incurring interest charges.

The misreported dates were traced to Pinal County. ASRS representatives contacted county representatives to inform them of this reporting error so that the county can correct it.

Recommendation:

The employer should report the correct pay period ending date for the accrual of compensation, rather than the payroll paid date.

Employer Response:

The District understands we are to use the pay period end dates for our ASRS reports. In Pinal County, the Pinal County School Office submits these reports on behalf of the Districts. I spoke to someone at Pinal County School Office Data Processing & they assured me that these reports are now being submitted using the pay period end dates.

FINDING 3:

Santa Cruz Valley Union High School District did not ensure that all retirees returning to work under A.R.S. §§ 38-766.01 and 38-766.02 complied with the requirement that they acknowledge the provisions of the statute in writing.

A.R.S. § 38-766.01 provides the guidelines for retirees who wish to return to work without suspension of benefits. A.R.S. § 38-766.01(C) states “the retired member shall acknowledge this section in writing and file the acknowledgement with the employer within thirty days of returning to work.”

The ASRS requires that employers provide a copy of this acknowledgement to the ASRS. A.R.S. § 38-766.02(E) states, “an employer of a retired member shall submit any reports, data, paperwork or materials that are requested by the ASRS.”

At the beginning of field work, the District had written documentation for some, but not all, of its retirees who had returned to work. Eleven retirees were working after retirement in direct employment. Eight of these did not have proper written documentation at the beginning of field work, and the District did not have any of these retired members complete proper forms before the end of field work.

Recommendation:

The District should ensure that all retirees working in direct employment complete the online return to work form, within 30 days of reemployment, to acknowledge in writing the conditions under which they are returning to work.

Employer Response:

The District has requested and is helping our return to work employees fill out the necessary form on line. The District had eight Return to Work employees on the audit listing. Five of the

ARIZONA STATE RETIREMENT SYSTEM
SANTA CRUZ VALLEY UNION HIGH SCHOOL DISTRICT
RECOMMENDATIONS

employees have finished their form online. The other three have been asked to get it completed as soon as possible. We have also offered to help with this process if they need help. Going forward, the District will explain to all return to work employees we might hire back that this form is a requirement before we can hire them back.

FINDING 4:

The Santa Cruz Valley Union High School District did not report all demographic information for its members.

A.R.S. § 38-715 establishes the requirements to maintain the books and processing records of the ASRS. A.R.S. § 38-737 says that employer contributions will be determined by the ASRS actuary every year. The actuary requires full demographic information in order to make an accurate calculation of the contribution rate.

The District reported contributions for 57 members in fiscal year 2015, most of whom had all required demographic information. At the beginning of the audit the District was informed that it had one member who had not enrolled in the ASRS and who was missing the following items of demographic information: date of birth, marital code, gender and address. The District was requested to have this member properly enroll, but was unable to do so because the member is no longer employed by the District. The error rate was under 2%.

Recommendation:

The District should ensure that all newly hired eligible members complete online enrollment prior to submitting contributions so that this information will be collected for all new employees.

Employer Response:

The District will go online every pay period to ensure all new employees have enrolled online with the Arizona State Retirement System.

St. David USD Audit

**A REPORT TO THE
ARIZONA STATE RETIREMENT SYSTEM
OPERATIONS AND AUDIT COMMITTEE**

**ARIZONA STATE RETIREMENT SYSTEM
EMPLOYER AUDITS**

ST. DAVID UNIFIED SCHOOL DISTRICT

MARCH 4, 2016

The audit of St. David Unified School District was completed March 4, 2016, for the period July 1, 2014 through June 30, 2015.

The preliminary audit objectives were to determine whether the St. David Unified School District is in compliance with Arizona Revised Statutes (A.R.S.) governing the following:

- Eligible compensation and required contributions reported to the ASRS.
- Accurate and timely enrollment of all eligible employees.
- Reporting and remitting of the employees' and employer's share of contributions.
- Medical and dental insurance premium benefits payable to retired employees.
- Retirees' return to work.

SUMMARY OF FINDINGS:

Based on the results of the work performed to meet the above audit objectives, the following statements summarize the findings presented to St. David Unified School District:

- 1. St. David Unified School District did not remit the alternate contribution due on all eligible wages for four of its returned to work retirees.**
- 2. St. David Unified School District did not timely inform the ASRS that one retired member was no longer covered through St. David's medical insurance resulting in ASRS premium benefit overpayments.**

BACKGROUND

St. David Unified School District joined the ASRS on July 1, 1966 by executing an Application and Social Security 218 Agreement. St. David Unified School District currently has approximately 58 employees contributing to the ASRS.

DESCRIPTION OF AUDIT WORK PERFORMED

The audit work completed consisted of an examination of the employer's payroll and personnel records for the time period July 1, 2014 through June 30, 2015. The auditor reviewed pertinent documentation and interviewed St. David Unified School District personnel from the Human Resources and Payroll departments. The auditor performed substantive tests of the employees' employment and payroll records to provide sufficient assurance that the employer is accurately reporting and remitting ASRS retirement and Long Term Disability (LTD) contributions. The following audit tests were performed:

- Review of the employer payroll records and related ASRS reports.
- Review of employees' time sheets and payroll records to determine eligibility.
- Review of the noncontributing employees' personnel and payroll records to determine compliance with the 20 hour, 20 week eligibility criteria.
- Review of the retired employees' medical and dental insurance premium benefit.

ARIZONA STATE RETIREMENT SYSTEM
ST. DAVID UNIFIED SCHOOL DISTRICT
MARCH 4, 2016

- Determine compliance with A.R.S. § 38-766.01 by reviewing the hours and weeks worked and other criteria of retired employees who returned to work.
- Determine compliance with A.R.S. § 38-766.02 requirement to pay an ACR on all retirees who have returned to work in any capacity.
- Other detailed testing as required to meet the audit objectives.

AUDITOR COMMENTS:

St. David Unified School District personnel were cooperative, informative and helpful in providing FYE 2015 time reports, payroll records, and other information necessary to effectively complete the ASRS audit. Audit findings and recommendations were discussed and issues resolved in a timely manner.

**A REPORT TO THE
ARIZONA STATE RETIREMENT SYSTEM
OPERATIONS AND AUDIT COMMITTEE**

**ARIZONA STATE RETIREMENT SYSTEM
EMPLOYER AUDITS**

ST. DAVID UNIFIED SCHOOL DISTRICT

FINDINGS AND RECOMMENDATIONS

MARCH 4, 2016

ARIZONA STATE RETIREMENT SYSTEM
ST. DAVID UNIFIED SCHOOL DISTRICT
RECOMMENDATIONS

FINDING 1:

St. David Unified School District did not remit the alternate contribution due on all eligible wages for four of its returned to work retirees.

A.R.S. § 38-766.02 provides the guidelines for payment of the alternate contribution rate (ACR) for retirees who work after retirement. According to the statute, “an employer shall pay contributions at an alternate contribution rate on behalf of a retired member who returns to work in any capacity in a position ordinarily filled by an employee.” The ACR is to be “applied to the compensation, gross salary or contract fee of a retired member who meets the requirements of this section.”

St. David Unified School District had four return to work retiree’s where no alternate contribution was remitted on all eligible wages.

The estimated alternate contribution due, excluding interest, as determined by this audit is as follows:

Total Gross Earnings	<u>\$17,821</u>
Total Estimated Alternate Contribution Due	<u>\$1,705</u>

Recommendation:

St. David Unified School District should contact its contributions accounting representative at the Arizona State Retirement System (ASRS) to make arrangements for payment, including interest, of the alternate contribution due.

Employer Response:

The District will remit payment of \$1,705.00 plus interest for retirees that had no alternate contribution taken out.

FINDING 2:

St. David Unified School District did not timely inform the ASRS that one retired member was no longer covered through St. David’s medical insurance resulting in ASRS premium benefit overpayments.

A.R.S. § 38-783 provides for the ASRS to pay part of the coverage premium of any health and accident insurance for each retired member if the member elects to participate in the coverage provided by the ASRS or elects to participate in a health and accident insurance program provided by an employer.

The May, 2015, ASRS health insurance premium benefit report was selected for review. As of May, 2015, there were seven retirees receiving an ASRS premium benefit. One of these retirees had ceased medical coverage September, 2014. St. David Unified School District has submitted information to the ASRS necessary to process the overpayment.

The premium benefit overpayment due the ASRS, as determined by this audit is as follows:

Total Premium Benefit Overpayment Due	<u>\$1,800.00</u>
----------------------------------------------	--------------------------

ARIZONA STATE RETIREMENT SYSTEM
ST. DAVID UNIFIED SCHOOL DISTRICT
RECOMMENDATIONS

Recommendation:

St. David Unified School District should develop a monthly process to reconcile all ASRS premium benefit payments to ensure coverage has not ceased. St. David Unified School District should timely notify the ASRS whenever a retiree's medical coverage has ceased.

Employer Response:

The District has submitted paper work to remove retiree from ASRS premium benefit.

Town of Oro Valley Audit

**A REPORT TO THE
ARIZONA STATE RETIREMENT SYSTEM
OPERATIONS AND AUDIT COMMITTEE**

**ARIZONA STATE RETIREMENT SYSTEM
EMPLOYER AUDITS**

TOWN OF ORO VALLEY

MARCH 23, 2016

The audit of the Town of Oro Valley was completed on March 23, 2016 for the period July 1, 2014 through June 30, 2015.

The preliminary audit objectives were to determine whether the Town of Oro Valley is in compliance with Arizona Revised Statutes (A.R.S.) governing the following:

- Eligible compensation and required contributions reported to the ASRS.
- Accurate and timely enrollment of all eligible employees.
- Reporting and remitting of the employees' and employer's share of contributions.
- Medical and dental insurance premium benefits payable to retired employees.
- Retirees' return to work.

SUMMARY OF FINDING:

Based on the results of the work performed to meet the above audit objectives, the following statement summarizes the finding presented to the Town of Oro Valley:

- 1. The Town of Oro Valley did not report full demographic information for five employees.**

BACKGROUND

The Town of Oro Valley joined the ASRS October 15, 1974 by executing an Application and Social Security 218 agreement. The Town of Oro Valley currently has approximately 217 employees contributing to the ASRS.

DESCRIPTION OF AUDIT WORK PERFORMED

The audit work completed consisted of an examination of the employer's payroll and personnel records for the time period July 1, 2014 to June 30, 2015. The auditor reviewed pertinent documentation and interviewed Town of Oro Valley personnel from the Human Resources and Payroll departments. The auditor performed substantive tests of the employees' employment and payroll records to provide sufficient assurance that the employer is accurately reporting and remitting ASRS retirement and Long Term Disability (LTD) contributions. The following audit tests were performed:

- Review of the employer payroll records and related ASRS reports.
- Review of employees' time and payroll records to determine eligibility.
- Review of the noncontributing employees' personnel and payroll records to determine compliance with the 20 hour, 20 week eligibility criteria.
- Review of the retired employees' medical and dental insurance premium benefit.
- Determine compliance with A.R.S. § 38-766.01 by reviewing the hours and weeks worked and other criteria of retired employees who returned to work.

ARIZONA STATE RETIREMENT SYSTEM
TOWN OF ORO VALLEY
MARCH 23, 2016

- Determine compliance with A.R.S. § 38-766.02 requirement to pay an ACR on all retirees who have returned to work in any capacity in a position ordinarily filled by an employee.
- Other detailed testing as required to meet the audit objectives.

AUDITOR COMMENTS:

Town of Oro Valley personnel were cooperative, informative and helpful in providing time reports, payroll records, and other information necessary to effectively complete the ASRS audit. Audit findings and recommendations were discussed and issues resolved in a timely manner.

**A REPORT TO THE
ARIZONA STATE RETIREMENT SYSTEM
OPERATIONS AND AUDIT COMMITTEE**

**ARIZONA STATE RETIREMENT SYSTEM
EMPLOYER AUDITS**

TOWN OF ORO VALLEY

FINDINGS AND RECOMMENDATIONS

MARCH 23, 2016

ARIZONA STATE RETIREMENT SYSTEM
TOWN OF ORO VALLEY
RECOMMENDATIONS

FINDING 1:

Town of Oro Valley did not report full demographic information for five employees.

A.R.S. § 38-715 establishes the requirements to maintain the books and processing records of ASRS. A.R.S. § 38-737 states that employer contributions will be determined by the ASRS actuary every year. The ASRS actuary requires full demographic information in order to make an accurate calculation of the contribution rate.

Recommendation:

Town of Oro Valley should continue to ensure that all eligible members complete online enrollment prior to submitting contributions in order for the ASRS to have full demographic information.

Employer Response:

The employer agreed.

Tucson Airport Authority Audit

**A REPORT TO THE
ARIZONA STATE RETIREMENT SYSTEM
OPERATIONS AND AUDIT COMMITTEE**

**ARIZONA STATE RETIREMENT SYSTEM
EMPLOYER AUDITS**

TUCSON AIRPORT AUTHORITY

JANUARY 28, 2016

The audit of Tucson Airport Authority was completed January 28, 2016 for the period July 1, 2014 through June 30, 2015.

The preliminary audit objectives were to determine whether the Tucson Airport Authority is in compliance with Arizona Revised Statutes (A.R.S.) governing the following:

- Eligible compensation and required contributions reported to the ASRS.
- Accurate and timely enrollment of all eligible employees.
- Reporting and remitting of the employees' and employer's share of contributions.
- Medical and dental insurance premium benefits payable to retired employees.
- Retirees' return to work.

SUMMARY OF FINDINGS:

Based on the results of the work performed to meet the above audit objectives, the following statement summarize the finding presented to Tucson Airport Authority:

- 1. The Tucson Airport Authority applied and remitted contributions on 17 employee's option to sell back accumulated leave.**

BACKGROUND

The Tucson Airport Authority joined the ASRS on July 1, 1962 by executing an Application and Social Security 218 Agreement. The Tucson Airport Authority currently has approximately 207 employees contributing to the ASRS.

DESCRIPTION OF AUDIT WORK PERFORMED

The audit work completed consisted of an examination of the employer's payroll and personnel records for the time period July 1, 2014 through June 30, 2015. The auditor reviewed pertinent documentation and interviewed Tucson Airport Authority personnel from the Human Resources and Payroll departments. The auditor performed substantive tests of the employees' employment and payroll records to provide sufficient assurance that the employer is accurately reporting and remitting ASRS retirement and Long Term Disability (LTD) contributions. The following audit tests were performed:

- Review of the employer payroll records and related ASRS reports.
- Review of employees' time sheets and payroll records to determine eligibility.
- Review of the noncontributing employees' personnel and payroll records to determine compliance with the 20 hour, 20 week eligibility criteria.
- Review of the retired employees' medical and dental insurance premium benefit.
- Determine compliance with A.R.S. § 38-766.01 by reviewing the hours and weeks worked and other criteria of retired employees who returned to work.

ARIZONA STATE RETIREMENT SYSTEM
TUCSON AIRPORT AUTHORITY
JANUARY 28, 2016

- Determine compliance with A.R.S. § 38-766.02 requirement to pay an ACR on all retirees who have returned to work in any capacity.
- Other detailed testing as required to meet the audit objectives.

AUDITOR COMMENTS:

The Tucson Airport Authority personnel were cooperative, informative and helpful in providing time reports, payroll records, and other information necessary to effectively complete the ASRS audit. Audit findings and recommendations were discussed and issues resolved in a timely manner.

**A REPORT TO THE
ARIZONA STATE RETIREMENT SYSTEM
OPERATIONS AND AUDIT COMMITTEE**

**ARIZONA STATE RETIREMENT SYSTEM
EMPLOYER AUDITS**

TUCSON AIRPORT AUTHORITY

FINDINGS AND RECOMMENDATIONS

January 28, 2016

ARIZONA STATE RETIREMENT SYSTEM
TUCSON AIRPORT AUTHORITY
RECOMMENDATIONS

FINDING 1:

The Tucson Airport Authority applied and remitted contributions on 17 employees' option to sell back accumulated leave.

A.R.S. § 38-711 paragraph 7 subdivision (c) states that compensation “does not include payment, at the members option, in lieu of fringe benefits that are normally paid for or provided by the employer.” Tucson Airport Authority remitted contributions on 17 employees who exercised their option to sell back accumulated leave.

The gross earnings and employer and employee contributions to be credited to the employer's account, as determined by this audit are as follows:

Total Gross Earnings	<u>\$93,688</u>
Member Contributions	10,801
Employer Contributions	10,801
Total Credit	<u>\$21,602</u>

Recommendations:

1. Tucson Airport Authority should contact its contributions accounting representative at ASRS to make arrangements to take this available credit.
2. Contributions should not be withheld on payments, at the employee's option, in lieu of fringe benefits that are normally paid for or provided by the employer.

Employer Response:

The Tucson Airport Authority received on January 25, 2016, the draft Audit Report of Tucson Airport Authority's compliance with Arizona State Retirement System (ASRS) statutes governing the following:

1. Arizona Revised Statutes (A.R.S.) governing member eligibility for and enrollment in the ASRS.
2. A.R.S. governing eligible compensation and required contributions reported to the ASRS.
3. A.R.S. governing reporting and remitting the employee and employer share of contributions.
4. A.R.S. governing health benefit supplement payments for retired employees.
5. A.R.S. governing return to work retirees.
6. A.R.S. governing employer termination incentive plans.

This report identified one finding, which states the Tucson Airport Authority applied and remitted contributions on seventeen employees' option to sell back accumulated leave. The Tucson Airport Authority accepts the finding as stated in the Audit Report and will coordinate with ASRS staff on appropriate follow-up actions.

ARIZONA STATE RETIREMENT SYSTEM
TUCSON AIRPORT AUTHORITY
RECOMMENDATIONS

We wish to thank Mr. Larry Rennaker, CPA and the staff of the Arizona State Retirement System for the professionalism and courtesies extended to the Tucson Airport Authority during the audit.

Sincerely,
TUCSON AIRPORT AUTHORITY

John M. Schubert, CPA
Senior Director of Finance and Information Technology/CIO

Agenda Item #4

**STATUS OF INTERNAL AUDITS
FOR THE 9 MONTHS ENDED (March 2016)**

2015/16 <u>AUDITS</u>	<u>HOURS BUDGETED</u>	<u>ACTUAL HOURS WORK YTD</u>	<u>PERCENT OF HOURS UTILIZED</u>	<u>ESTIMATED</u>		<u>EXPLANATION OF ACTUAL HOURS THAT EXCEED BUDGET BY MORE THAN 10%</u>
				<u>HOURS REMAINING</u>	<u>TOTAL HOURS WHEN COMPLETE</u>	
Service Purchase Invoices	150	118	79%	32	150	
Investment Trade Tickets	0	0	0%	0	0	
Fraud Hotline/Internal Investigations	200	108	54%	92	200	
Employer Audits	3,200	2,909	91%	291	3,200	
Pension/Survivor Final Audit	200	199	100%	1	200	
Refunds Processing	150	118	79%	32	150	
Audit Follow-up	150	160	107%	0	160	
Census Data GASB 68	300	318	106%	0	318	
Software Licensing	150	160	107%	0	160	
WEB Services Post Implementation	450	0	0%	0	0	
Procurement Bid Process	0	0	0%	0	0	Removed from audit plan
Management Fees-Agency	500	100	20%	400	500	
QDROs	100	100	100%	0	100	
TOTALS	5,550	4,290		1,298	5,588	
OTHER THAN AUDITS						
Member Statement Testing	100	105	105%	0	105	
Director Requests	200	45	23%	155	200	
Requested Audits/Other*	200	0	0%	200	200	
TOTALS	500	150		355	505	
GRAND TOTAL	6,050	4,440		1,653	6,093	

Agenda Item #5A



ARIZONA STATE RETIREMENT SYSTEM

3300 NORTH CENTRAL AVENUE • PO BOX 33910 • PHOENIX, AZ 85067-3910 • PHONE (602) 240-2000
4400 EAST BROADWAY BOULEVARD • SUITE 200 • TUCSON, AZ 85711-3554 • PHONE (520) 239-3100
TOLL FREE OUTSIDE METRO PHOENIX AND TUCSON 1 (800) 621-3778

Paul Matson
Director

MEMORANDUM

TO: Mr. Jeff Tyne, Chair, Operations and Audit Committee (OAC)

FROM: Mr. Anthony Guarino, Deputy Director and Chief Operations Officer
Enterprise Risk Management (ERM) Committee

DATE: March 31, 2016

RE: **Agenda Item #5.A.:** Presentation, Discussion and Appropriate Action Regarding the ASRS Internal IT Risk Assessment

Purpose

Staff will provide the OAC with a risk assessment focusing on the agency network applications, hardware and upgrade and continuity of operations functions and the strategic goal to provide members and business users with technology that is high performing, secure, and able to support evolving business needs.

Recommendation

Informational only, no action required.

Background

Since 2007, the ASRS has conducted risk assessments and devised control strategies based on principles espoused by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission. The COSO reports, *Enterprise Risk Management – Integrated Framework: Executive Summary Framework*, dated September 2004 and *Internal Control – Integrated Framework: Framework and Appendices*, dated May 2013, are considered authoritative sources and promote an enterprise-wide, integrated risk management approach. The principles, as adopted by the ASRS, are intended to provide the ASRS Director and Board reasonable assurance the ASRS is taking appropriate steps to manage and mitigate risk according to its priorities.

The ASRS has organized an Enterprise Risk Management (ERM) Steering Committee, led by the Deputy Director and Chief Operations Officer and staffed with senior managers, to take an iterative approach and continuously assess the risks and threats facing the agency. Committee decisions and activities are monitored by the agency's Chief Internal Auditor, who has a direct reporting relationship with the ASRS Director and OAC Chair.

The ERM Committee's most recent focus has been on risks that threaten agency network applications, hardware and upgrades and continuity of operations.

Enterprise Risk Management (ERM) OAC Presentation

Focus on Agency Network Applications,
Security
And Continuity of Operations

April 2016

Section One

Strategic Goal and Objectives

ASRS Strategic Goal #10:

Provide members and business users with technology that is high performing, secure, and able to support evolving business needs

Business functions included in Goal #10:

- Business Applications Development, Maintenance, and Upgrades (not addressed in this presentation)
- Continuity of Operations (COOP)
- Maintain Network Applications, Hardware, and Upgrades

ASRS Strategic Objectives:

Risk Mitigation

1. In conjunction with the agency risk management program, take appropriate steps and provide reasonable assurance to Executive Management and the Board that technology is high-performing, secure, and able to support evolving business needs

Maintain Network Applications, Hardware, and Upgrades

1. Present a schedule to Senior Managers prior to the start of each fiscal year of network hardware and software maintenance and upgrades recommended for implementation in the upcoming fiscal year. The schedule should include the reason for the upgrade, the estimated timeframe for implementation, additional costs to the agency, business resources required, and any risks to the agency associated with implementing, or not implementing, the upgrade.
2. Implement 90 percent or more of hardware and software upgrades that have been scheduled for implementation during the fiscal year.
3. Ensure that telephone systems are available 98 percent or higher of the time.
4. Ensure critical business applications are available 97 percent or higher of the time.
5. Ensure network applications are available 99 percent or higher of the time.
6. Maintain a helpdesk satisfaction rating of 90 percent or higher.

Continuity of Operations Plan (COOP)

1. Conduct an annual COOP functionality test, and one or more tabletop exercises.
2. In the event of business emergency, ensure that the crisis management team is capable of activating the COOP within 2 hours of notification, and, once activated, can:
 - a) Restore telephone systems within 10 hours.
 - b) Restore critical business applications within 24 hours.
 - c) Restore network applications within 24 hours.

Section Two (Executive Summary)

Significant Risks and Control Strategies

Significant Risks and Strategies – Network Applications

Risk/Threat	Risk Rankings		Control Evaluation as of March 2016	Management Strategy for risk and Internal Audit
<p>2. Information systems are not secure from external threats or electronic intrusions, including illegal, unethical, or fraudulent data manipulation, financial disbursements, and identity theft</p>	<p>Tolerance: Low</p>	<p>Impact: Major</p>	<p>Current Controls: Operations geared toward meeting clearly defined NIST standards, overseen and supported by ERM. Activities and tools to ensure adequate maturity levels and secure externally facing systems include:</p> <ul style="list-style-type: none"> a. Next generation firewalls b. Web filtering c. Web application firewalls d. Network management tool e. Vulnerability management f. Application and device control for PC g. Third party patch management h. Data loss prevention software for email i. End point protection on PC and servers j. Log event managing system k. Administrative controls l. Independent network monitoring m. Biennial external security assessment and remediation activities n. Biennial Internal Audit to ensure compliance with external assessment recommendations o. Full disk encryption for laptops and thumb drives p. Some policies and procedures in place q. Schedules are in place to replace hardware and software r. Inventory controls in place s. Some whitelisting (stops unauthorized installation/execution) in place t. Database audit vault (for forensics). 	<p>Reduce the anticipated risk levels</p> <p>IA should continue biennial compliance audit</p>

Significant Risks and Strategies (continued)

Risk/Threat	Risk Rankings		Control Evaluation as of March 2016	Management Strategy for risk and Internal Audit
2. Continued from prior page	Controls: Some Vulnerability	Likelihood: Some Likelihood	Future Actions: <ul style="list-style-type: none"> Review and update 5-Year Plan to achieve targeted Gartner Security Maturity models and incorporate findings from 2016 security assessment. Prioritize and complete actions identified in 5-Year Plan Security resource positions recruitment underway 	Reduce the anticipated risk levels
3. Information systems are not secure from internal threats or physical intrusions, including illegal, unethical, or fraudulent data manipulation, financial disbursements, and identity theft	Tolerance: Low	Impact: Major	Current Controls: Operations geared toward meeting clearly defined NIST standards, overseen and supported by ERM. Web filtering blocks malicious websites from staff. Employees and contractors sign a security agreement annually as well as attending annual security awareness training. Telecommuting employees are made aware of the risks and consequences and sign an agreement. Agency follows the recommended Remediation Roadmap from the biennial Information Security Assessment Reports and conducts annual or biennial external compliance assessments. Security documentation has been standardized on the NIST framework. Code reviews are performed. Software is used to discover new network risks. Risk mitigation strategies include: <ul style="list-style-type: none"> See response to #2 Badging system, policy and procedures, and restrictions to ASRS floors Secure File Transfer Physical access restrictions and monitoring (i.e. cameras, panic buttons, updated access reporting) Key Control Program New ASRS employees undergo background checks 	Reduce the anticipated risk levels

Significant Risks and Strategies (continued)

Risk/Threat	Risk Rankings		Control Evaluation as of March 2016	Management Strategy for risk and Internal Audit
3. Continued from prior page	Controls: Some Vulnerability	Likelihood: Some Likelihood	Future Actions: <ul style="list-style-type: none"> • Achieve targeted Gartner Security Maturity levels. • Security resource positions recruitment underway. • Prioritize and complete actions identified in 5-Year Plan including actions directed toward telecommuting 	Reduce the anticipated risk levels
4. Information systems, applications, and data are not recoverable from system outages, physical loss, and/or malicious intrusion (like ransomware), etc.	Tolerance: Low	Impact: Major	Current Controls: Operations geared toward meeting clearly defined NIST standards, overseen and supported by ERMC. Continuity of Operations Plan ensures information systems, applications, and data are recoverable. ASRS uses a dual method of backup of its data systems disk to tape and disk to disk. Backup tapes are sent to an offsite location. Mirroring of key databases and files are being completed to our off-site facility. We have been following an equipment refresh schedule to ensure all systems are supported and meet the needs of the agency. Periodic restoration tests of back-ups to ensure integrity of data.	Reduce the anticipated risk levels
	Controls: Some Vulnerability	Likelihood: Some Likelihood	Future Actions: <ul style="list-style-type: none"> • Achieve targeted Gartner Security Maturity levels. • The back-up cycle should be reviewed for sufficiency and reviewed in conjunction with the data retention policy • Equipment upgrades are planned. • Strategy to bring data back from alternate site to Phoenix still being researched 	

Significant Risks and Strategies (continued)

Risk/Threat	Risk Rankings		Control Evaluation as of March 2016	Management Strategy for risk and Internal Audit
6. Non-secure email containing PII is sent	Tolerance: Low	Impact: Major	Current Controls: Operations geared toward meeting clearly defined NIST standards, overseen and supported by ERM. Control software (an email inspection tool and secure file transfer) in place. Role based access controls in place. Annual security training is provided to staff.	Evaluate the anticipated risk levels
	Controls: Some Vulnerability	Likelihood: Some Likelihood	Future Actions: <ul style="list-style-type: none"> • Achieve targeted Gartner Security Maturity levels. • Management should evaluate whether additional controls should be implemented 	

Significant Risks and Strategies_(continued)

Risk/Threat	Risk Rankings		Control Evaluation as of March 2016	Management Strategy for risk and Internal Audit
7. Unauthorized information containing non-PII sensitive data is released	Tolerance: Low	Impact: Major	<p>Current Controls: Operations geared toward meeting clearly defined NIST standards, overseen and supported by ERM. Web filtering blocks malicious websites from staff. Employees and contractors sign a security agreement annually as well as attending annual security awareness training. Telecommuting employees are made aware of the risks and consequences and sign an agreement. Agency follows the recommended Remediation Roadmap from the biennial Information Security Assessment Reports and conducts annual or biennial external compliance assessments. Security documentation has been standardized on the NIST framework. Software is used to discover new network risks. Risk mitigation strategies include:</p> <ul style="list-style-type: none"> • See response to #2 • Badging system, policy and procedures, and restrictions to ASRS floors • Secure File Transfer • Physical access restrictions and monitoring (i.e. cameras, panic buttons, updated access reporting) • Key Control Program • New ASRS employees undergo background checks • Role based access controls 	Evaluate the anticipated risk levels
	Controls: Some Vulnerability	Likelihood: Some Likelihood	<p>Future Actions:</p> <ul style="list-style-type: none"> • Achieve targeted Gartner Security Maturity levels. • Management should: <ul style="list-style-type: none"> • Evaluate whether additional controls should be implemented: <ul style="list-style-type: none"> • Implement access audits and DLP as per 5-Year Plan • Determine if sensitive data is defined 	

Significant Risks and Strategies (continued)

Risk/Threat	Risk Rankings		Control Evaluation as of March 2016	Management Strategy for risk and Internal Audit
24. A system breach goes undetected for a period of time	Tolerance: Low	Impact: Major	Current Controls: Operations geared toward meeting clearly defined NIST standards, overseen and supported by ERM. Forensic data capture is in place including back-ups, system logging, and database audit vault. Notifications of vulnerabilities are received from external and internal entities. Resources are redirected to address threats. Industry standard devices and practices are utilized within ASRS IT environment. Processes and procedures are in place to remediate vulnerabilities. Automatic updating of threat definitions on various security appliances. Cyber risk insurance is in place.	Reduce the anticipated risk levels
	Controls: Some Vulnerability	Likelihood: Some Likelihood	Future Actions: <ul style="list-style-type: none"> • Achieve targeted Gartner Security Maturity levels. • Additional measures will be implemented under the 5 year plan • Recruitment is underway for additional security resources 	

Significant Risks and Strategies-coop

Risk/Threat	Risk Rankings		Control Evaluation as of March 2016	Management Strategy for risk and Internal Audit
<p>2. Business continuity plans are not established, tested, reviewed or sufficient to support business operations in the event of a disaster</p>	<p>Tolerance: Low</p>	<p>Impact: Major</p>	<p>Current Controls: Periodic comprehensive tests are performed to evaluate the ability to recover core business systems at our alternate site should a short duration incident occur. IMD's COOP is integrated into overall agency COOP. The Business Impact Assessment (BIA) is periodically reviewed and updated to verify threats, recovery time objectives, and disaster recovery (DR) staffing requirements. Internal Audit monitors COOP tests and consults as necessary. COOP plan is housed with Department of Emergency and Military Affairs (DEMA).</p>	<p>Accept the anticipated risk levels</p>
	<p>Controls: Strong</p>	<p>Likelihood: Not Likely</p>	<p>Future Actions: COOP update is underway</p>	

Section Three

Ranking Criteria

Rankings: IMPACT

Measures the impact should the risk occur

Minor

Indicates a risk occurrence would create no noticeable:

Disruption to normal operations

- Disruption to existing systems:
 - Phones, network, POL, PERIS, FileNet down for up to 4 hours
 - Website down for up to 24 hours
 - MUNIS down for up to 1 week
- System security successfully defended
- System performance slower than normal but does not disrupt normal operations

Disruption to strategic technology development

- Project and production support delays have a 10 - 20% negative impact to annual project plan
- <10% negative variance to outcome user satisfaction

Financial impact

- Current budget year can absorb the equipment, resource, software and licensing costs

Reputation/public image damage

- No inquiries from media/government agencies
- No loss of stakeholder trust in ASRS

Moderate

Indicates a risk occurrence could create a modest:

Disruption to normal operations

- Disruption to existing systems:
 - Phones, network, POL, PERIS, FileNet down for 4 - 8 hours
 - Website down for 25 - 48 hours
 - MUNIS down for 8 - 31 days
- System security partially compromised but no loss occurs
- System performance impedes non-critical objectives
- COOP team assembled but not activated

Disruption to strategic technology development

- Project and production support delays have a 21 - 30% negative impact to annual project plan
- 11 - 20% negative variance to outcome user satisfaction

Financial impact

- Current budget year can partially absorb the equipment, resource, software and licensing costs

Reputation/public image damage

- Public statement issued
- Some loss of stakeholder trust in ASRS

Major

Indicates a risk occurrence could create a significant:

Disruption to normal operations

- Disruption to existing systems:
 - Phones, network, POL, PERIS, FileNet down for >8 hours
 - Website down for >48 hours
 - MUNIS down for >31 days
- System security significantly compromised and loss occurs
- System performance impedes critical objectives
- COOP plan is activated

Disruption to strategic technology development

- Project and production support delays have a >30% negative impact to annual project plan
- >21% negative variance to outcome user satisfaction

Financial impact

- Current budget year cannot absorb the equipment, resource, software and licensing costs

Reputation/public image damage

- Media coverage
- Results in legislation and/or lawsuits that set precedent
- Loss of stakeholder trust in ASRS

Rankings: CONTROLS

Strengthen controls to lessen risk

Strong

Indicates the controls in place are strong and will mitigate manageable risk

- Duties and responsibilities are clearly delineated between the Board and Director
- Staff engagement with the OAC ensures appropriate oversight
- Senior Management establishes priorities and schedules and CCB provides oversight
- Goals and objectives are clearly defined and supported by the organizational structure
- Staff engagement with ADOA (ASET) ensures adequate collaboration and timely approval of technology investment
- Established methodology (i.e. Agile SCRUM) to develop software
- Technology software/hardware in place is updated/upgraded to support business processes and ensure adequate security
- Performance is analyzed, measured, reported
- Staff duties are properly segregated and responsibilities defined
- SMEs in place
- Rules, policies, SOPs in place
- Communication channels established
- IA and external auditors test control adequacy and staff follows up
- Enterprise Risk Management Committee functions as IT security steering committee

Some Vulnerability

Indicates the controls in place have areas of vulnerability that may not, or may not always, mitigate manageable risk

- Missing some elements of strong controls
- External factors that create technology security risks may be evolving faster than the agency can mitigate
- Constraints on independence and autonomy may impede the agency's ability to mitigate some risks in a timely fashion
- Not all elements of proper governance are in place

Weak

Indicates the controls in place are not adequate to mitigate manageable risk

- Missing many elements of strong controls
- Subject matter expertise is substandard
- Goals and objectives are unclear
- Internal Audit does not verify the adequacy of controls
- Performance is not analyzed, measured, or reported
- External factors that create technology security risks are known to be evolving faster than the agency can mitigate
- Constraints on independence and autonomy impede the agency's ability to mitigate many risks in a timely fashion
- Proper governance not in place

Rankings: TOLERANCE

High	Medium	Low
<p>Indicates a general acceptance of risk usually because the likelihood of a risk event with a major impact is small</p>	<p>Indicates an acceptance that a risk event could occur because the cost or effort for stronger controls may outweigh benefit</p>	<p>Indicates the risk should be eliminated to the extent possible because of a low risk appetite or the likelihood of major impact</p>

Rankings: LIKELIHOOD

Probability that the risk identified would or would not occur

Not Likely	Some Likelihood	Likely
<p>Indicates the risk will probably not occur</p> <ul style="list-style-type: none"> • Risk event can usually be controlled • Strong controls/low tolerance • Not likely to occur in the next year 	<p>Indicates there is some probability the risk will occur</p> <ul style="list-style-type: none"> • Risk event cannot always be controlled • Missing some elements of strong controls/some tolerance • Some likelihood to occur in the near term if unchecked 	<p>Indicates it is probable the risk will occur</p> <ul style="list-style-type: none"> • Risk event cannot be controlled • Missing numerous elements of strong controls/high tolerance • Likely to happen if unchecked

Appendix A

Enterprise Risk Management Process

Enterprise Risk Management

- ▶ **Enterprise Risk Management (ERM) Committee:**
 - Led by the Deputy Director and comprised of Senior Managers
 - Under the oversight of the OAC
 - Communicates activities and findings to the Director
 - Works collaboratively with Internal Audit
 - Produces risk assessments and control strategies

- ▶ **Risk:** Any event that impacts, impedes, or interferes with the agency's ability to achieve its strategic priorities, goals, and objectives

- ▶ Risk management process conducted in accordance with principles espoused by the Committee of Sponsoring Organizations (COSO)

"Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

COSO Components of ERM

- ▶ **Control Environment** (Board, Executive and Senior Management set tone, philosophy, risk appetite)
- ▶ **Risk Assessment** (Iterative process for identifying/analyzing risks to achieving goals/objectives and determining how risks should be managed)
- ▶ **Control Activities** (Actions established to ensure risk mitigation)
- ▶ **Information and Communication** (Enables the Board, management, staff, and other stakeholders to understand internal control responsibilities and day-to-day control activities)
- ▶ **Monitoring** (Ongoing evaluations to ensure internal control components are present and functioning)

COSO Framework - May 2013

Risk Assessment Steps

- ▶ The risk assessment document groups major functions according to the agency's strategic plan
- ▶ **Workgroups** [comprised of Senior Managers and subject matter experts (SMEs)]:
 - Identify risks to achieving the strategic goals and objectives
 - Rank the risks and controls using a heat chart
 - Identify current risk control strategies
 - Identify control strategies under development/consideration
- ▶ **ERM Committee:**
 - Establishes the control environment, including the general internal control structure, tolerance levels, and risk parameters (impacts, likelihood)
 - Reviews the findings of SME workgroups; identifies control gaps
 - Ensures risk mitigation responsibilities and strategies are clearly identified
 - Monitors administration and progress
- ▶ Director and OAC receive periodic updates from the ERM Committee

Appendix B

Risk Assessment for Maintain Network
Applications, Hardware, and Upgrades
AND
Continuity of Operations

Maintain Network Applications, Hardware, and Upgrades

Risk/Threat	Risk Rankings		Control Evaluation – March 2016	Management Strategy for risk and IA
<p>1. Fail to utilize effective project management for new projects, and upgrades</p>	<p>Tolerance: Medium</p>	<p>Impact: Moderate</p>	<p>Current Controls: Project management resources, JIRA and project dashboards are utilized. State and PMP certified project managers are on staff. Oversight is provided by the Senior Management Team, Change Control Board, Executive Management Team, Operations and Audit Committee, Enterprise Risk Management Committee and ASET. Project managers utilize the PMBOK principles and guidelines. For new development and upgrades, project managers are assigned to coordinate activities. Staff utilizes Agile methodology to complete projects. TSD utilizes project management and development tools to manage scope, schedule, cost and resources. Changes are presented to SMT for approval.</p>	<p>Reduce the anticipated risk levels</p>
	<p>Controls: Some Vulnerability</p>	<p>Likelihood: Some Likelihood</p>	<p>Future Actions:</p> <ul style="list-style-type: none"> • Over the next two years NIS will develop measures to establish and track priorities • Management should consider: <ul style="list-style-type: none"> ○ Analyze ways to mitigate resource constraints in order to create greater focus on projects (pulled from projects to Production Support) 	

Risk/Threat	Risk Rankings		Control Evaluation – March 2016	Management Strategy for risk and IA
<p>2. Information systems are not secure from external threats or electronic intrusions, including illegal, unethical, or fraudulent data manipulation, financial disbursements, and identity theft.</p>	<p>Tolerance: Low</p>	<p>Impact: Major</p>	<p>Current Controls: Operations geared toward meeting clearly defined NIST standards, overseen and supported by ERMC. Activities and tools to ensure adequate maturity levels and secure externally facing systems include:</p> <ul style="list-style-type: none"> a. Next generation firewalls b. Web filtering c. Web application firewalls d. Network management tool e. Vulnerability management f. Application and device control for PC g. Third party patch management h. Data loss prevention software for email i. End point protection on PC and servers j. Log event managing system k. Administrative controls l. Independent network monitoring m. Biennial external security assessment and remediation activities n. Biennial Internal Audit to ensure compliance with external assessment recommendations o. Full disk encryption for laptops and thumb drives p. Some policies and procedures in place q. Schedules are in place to replace hardware and software r. Inventory controls in place s. Some whitelisting (stops unauthorized installation/execution) in place t. Database audit vault (for forensics) 	<p>Reduce the anticipated risk levels</p> <p>IA should continue biennial compliance audit</p>

Risk/Threat	Risk Rankings		Control Evaluation – March 2016	Management Strategy for risk and IA
	Controls: Some Vulnerability	Likelihood: Some Likelihood	Future Actions: <ul style="list-style-type: none"> • Review and update 5-Year Plan to achieve targeted Gartner Security Maturity models and incorporate findings from 2016 security assessment. • Prioritize and complete actions identified in 5-Year Plan • Security resource positions recruitment underway 	

Risk/Threat	Risk Rankings		Control Evaluation – March 2016	Management Strategy for risk and IA
<p>3. Information systems are not secure from internal threats or physical intrusions, including illegal, unethical, or fraudulent data manipulation, financial disbursements, and identity theft</p>	<p>Tolerance: Low</p>	<p>Impact: Major</p>	<p>Current Controls: Operations geared toward meeting clearly defined NIST standards, overseen and supported by ERM. Web filtering blocks malicious websites from staff. Employees and contractors sign a security agreement annually as well as attending annual security awareness training. Telecommuting employees are made aware of the risks and consequences and sign an agreement. Agency follows the recommended Remediation Roadmap from the biennial Information Security Assessment Reports and conducts annual or biennial external compliance assessments. Security documentation has been standardized on the NIST framework. Code reviews are performed. Software is used to discover new network risks. Risk mitigation strategies include:</p> <ul style="list-style-type: none"> • See response to #2 • Badging system, policy and procedures, and restrictions to ASRS floors • Secure File Transfer • Physical access restrictions and monitoring (i.e. cameras, panic buttons, updated access reporting) • Key Control Program • New ASRS employees undergo background checks 	<p>Reduce the anticipated risk levels</p>

Risk/Threat	Risk Rankings		Control Evaluation – March 2016	Management Strategy for risk and IA
	Controls: Some Vulnerability	Likelihood: Some Likelihood	Future Actions: <ul style="list-style-type: none"> • Achieve targeted Gartner Security Maturity levels. • Security resource positions recruitment underway. • Prioritize and complete actions identified in 5-Year Plan including actions directed toward telecommuting 	
4. Information systems, applications, and data are not recoverable from system outages, physical loss, and/or malicious intrusion (like ransomware), etc.	Tolerance: Low	Impact: Major	Current Controls: Operations geared toward meeting clearly defined NIST standards, overseen and supported by ERM. Continuity of Operations Plan ensures information systems, applications, and data are recoverable. ASRS uses a dual method of backup of its data systems disk to tape and disk to disk. Backup tapes are sent to an offsite location. Mirroring of key databases and files are being completed to our off-site facility. We have been following an equipment refresh schedule to ensure all systems are supported and meet the needs of the agency. Periodic restoration tests of back-ups to ensure integrity of data.	Reduce the anticipated risk levels

Risk/Threat	Risk Rankings		Control Evaluation – March 2016	Management Strategy for risk and IA
	Controls: Some Vulnerability	Likelihood: Some Likelihood	Future Actions: <ul style="list-style-type: none"> • Achieve targeted Gartner Security Maturity levels. • The back-up cycle should be reviewed for sufficiency and reviewed in conjunction with the data retention policy • Equipment upgrades are planned. • Strategy to bring data back from alternate site to Phoenix still being researched 	
5. Proper sanitation of equipment is not performed prior to disposal causing an exposure and/or loss of data	Tolerance: Low	Impact: Moderate	Current Controls: Operations geared toward meeting clearly defined NIST standards, overseen and supported by ERMC. All hard drives are removed from devices prior to disposal and shredded by a third party vendor. Prior to being sold as surplus, items require a TSD certification in writing of proper cleansing prior to disposal by Procurement. Updated Surplus Property SOP in place and is adhered to. Only encrypted printer drives are used and the destruction software is purchased at the same time the printer is purchased; additionally the hard drives are removed and shredded prior to disposal. Every surplus pick up is witnessed by TSD staff. A degausser has been purchased.	Accept the anticipated risk levels

Risk/Threat	Risk Rankings		Control Evaluation – March 2016	Management Strategy for risk and IA
	Controls: Strong	Likelihood: Not Likely	Future Actions: <ul style="list-style-type: none"> • Achieve targeted Gartner Security Maturity levels. • Shredding procedures for hard drives should be implemented • Developing a process for data destruction using the degausser 	
6. Non-secure email containing PII is sent	Tolerance: Low	Impact: Major	Current Controls: Operations geared toward meeting clearly defined NIST standards, overseen and supported by ERMC. Control software (an email inspection tool and secure file transfer) in place. Role based access controls in place. Annual security training is provided to staff.	Evaluate the anticipated risk levels
	Controls: Some Vulnerability	Likelihood: Some Likelihood	Future Actions: <ul style="list-style-type: none"> • Achieve targeted Gartner Security Maturity levels. • Management should evaluate whether additional controls should be implemented. 	

Risk/Threat	Risk Rankings		Control Evaluation – March 2016	Management Strategy for risk and IA
<p>7. Unauthorized information containing non-PII sensitive data is released</p>	<p>Tolerance: Low</p>	<p>Impact: Major</p>	<p>Current Controls: Operations geared toward meeting clearly defined NIST standards, overseen and supported by ERM. Web filtering blocks malicious websites from staff. Employees and contractors sign a security agreement annually as well as attending annual security awareness training. Telecommuting employees are made aware of the risks and consequences and sign an agreement. Agency follows the recommended Remediation Roadmap from the biennial Information Security Assessment Reports and conducts annual or biennial external compliance assessments. Security documentation has been standardized on the NIST framework. Software is used to discover new network risks. Risk mitigation strategies include:</p> <ul style="list-style-type: none"> • See response to #2 • Badging system, policy and procedures, and restrictions to ASRS floors • Secure File Transfer • Physical access restrictions and monitoring (i.e. cameras, panic buttons, updated access reporting) • Key Control Program • New ASRS employees undergo background checks • Role based access controls 	<p>Evaluate the anticipated risk levels</p>

Risk/Threat	Risk Rankings		Control Evaluation – March 2016	Management Strategy for risk and IA
	Controls: Some Vulnerability	Likelihood: Some Likelihood	Future Actions: <ul style="list-style-type: none"> • Achieve targeted Gartner Security Maturity levels. • Management should: <ul style="list-style-type: none"> ○ Evaluate whether additional controls should be implemented: <ul style="list-style-type: none"> ▪ Implement access audits and DLP as per 5-Year Plan ○ Determine if sensitive data is defined 	
8. Not enough technical resources (people and tools) to meet strategic objectives, State standards, and targeted Gartner maturity levels	Tolerance: Low	Impact: Major	Current Controls: Operations geared toward meeting clearly defined NIST standards, overseen and supported by ERMC. Focused subgroups (Security, Tier I HelpDesk and Tier II Networking) have been established to manage the individual tasks. Cross-training has been increased for all networking activities. Formalized remediation of scan results and an enhanced patch management strategy have been implemented. Security training provided for development and testing. Schedules are coordinated with resource availability.	Reduce the anticipated risk levels

Risk/Threat	Risk Rankings		Control Evaluation – March 2016	Management Strategy for risk and IA
	Controls: Some Vulnerability	Likelihood: Some Likelihood	Future Actions: <ul style="list-style-type: none"> • Achieve targeted Gartner Security Maturity levels. Working through our 5 year plan to implement NIST controls and ensure compliance. • Recruitment for additional security personnel underway • Management should consider additional security training for appropriate personnel • See response to #1 	
9. SOPs are inadequate or not in place (seldom used processes not covered)	Tolerance: Medium	Impact: Minor	Current Controls: Operations geared toward meeting clearly defined NIST standards, overseen and supported by ERM. Where applicable, procedures are available to map to NIST standards. Some SOPs are in place. The desk procedures are reviewed and updated as needed (when HelpDesk tickets are resolved, when infrastructure changes are made, etc.).	Reduce the anticipated risk levels
	Controls: Some Vulnerability	Likelihood: Some Likelihood	Future Actions: <ul style="list-style-type: none"> • Achieve targeted Gartner Security Maturity levels. Working through our 5 year plan to implement NIST controls and ensure compliance. • Gaps in SOPs will be identified and addressed at least annually. • An overall security policy detailing security controls is under development. 	

Risk/Threat	Risk Rankings		Control Evaluation – March 2016	Management Strategy for risk and IA
10. Processing speed is not meeting business needs	Tolerance: Medium	Impact: Minor	Current Controls: TSD evaluates business needs when determining the adequacy of technology. Response times are now addressed in project charters and evaluated by the CCB as needed. Any degradation of speed is reported to HelpDesk and appropriate action is taken. Users have established communications channels if issues arise.	Accept the anticipated risk levels
	Controls: Some Vulnerability	Likelihood: Some Likelihood	Future Actions: No additional actions planned.	
11. SMT does not receive timely/sufficient information about progress made to the remediation plan, planned upgrades, and security profile to make informed decisions	Tolerance: Medium	Impact: Minor	Current Controls: Operations geared toward meeting clearly defined NIST standards, overseen and supported by ERM. Regular meetings to assess security vulnerabilities, end of life support, and systems compatibility are held in TSD to determine needed upgrades. A regular schedule is established to present findings/recommendations to Senior Management. Unanticipated upgrades are presented to SMT as needed. Communications channels are established to assess and address budget needs.	Reduce the anticipated risk levels
	Controls: Some Vulnerability	Likelihood: Some Likelihood	Future Actions: <ul style="list-style-type: none"> Enhance dashboards for future CCB presentations (remediation plans, planned upgrades and security profile) 	

Risk/Threat	Risk Rankings		Control Evaluation – March 2016	Management Strategy for risk and IA
12. Telephone system could experience a hardware/software failure	Tolerance: Low	Impact: Moderate	<p>Current Controls: Current system is managed by AZNET. Statewide service level agreements are in place and communication channels with AZNET are established. An escalation process is in place if any issues arise. Hardware has built-in redundancy to guard against failure. For members and employers, the ASRS has alternate methods of communication such as email, website, mail, etc. Downtime is tracked.</p>	Evaluate the anticipated risk levels
	Controls: Some Vulnerability	Likelihood: Some Likelihood	<p>Future Actions:</p> <ul style="list-style-type: none"> • Monitor and resolve problem resolution gap and report monthly to CCB 	
13. Telephone carrier may experience an outage	Tolerance: Low	Impact: Moderate	<p>Current Controls: Current system is managed by AZNET. Service level agreements are in place and communication channels with AZNET are established. An escalation process is in place if any issues arise. Carriers have redundancy to guard against outages. For members and employers, the ASRS has alternate methods of communication such as email, website, mail, etc.</p>	Accept the anticipated risk levels
	Controls: Strong	Likelihood: Not Likely	<p>Future Actions: No additional actions planned</p>	

Risk/Threat	Risk Rankings		Control Evaluation – March 2016	Management Strategy for risk and IA
<p>14. Hardware (servers, switches, etc.) failures may occur resulting in loss of productivity</p>	Tolerance: Medium	Impact: Moderate	<p>Current Controls: Some components have built-in redundancy to guard against failure. A stable, virtualized environment helps prevent outages and makes recovery faster. A disaster recovery site has been established and is regularly tested. Alerts will notify designated staff in the event of a failure. A refresh schedule is followed. Single points of failure have been identified and mitigated to tolerance. Maintain hardware support and replace prior to end of life.</p>	<p>Accept the anticipated risk levels</p>
	Controls: Some Vulnerability	Likelihood: Some Likelihood	<p>Future Actions: No additional actions planned</p>	
<p>15. Software application failures may occur resulting in loss of productivity and performance, etc.</p>	Tolerance: Low	Impact: Minor	<p>Current Controls: Operations geared toward meeting clearly defined NIST standards, overseen and supported by ERM. System and user acceptance tests are run prior to releasing new software. Database redundancy is established. Vendor support is in place. A stable, virtualized environment helps prevent outages and makes recovery faster. A disaster recovery site has been established and is regularly tested. Alerts will notify designated staff in the event of a failure. An established configuration management process is in place for software releases. A process is in place to rollout patches to prevent application failures.</p>	<p>Accept the anticipated risk levels</p>
	Controls: Strong	Likelihood: Some Likelihood	<p>Future Actions:</p> <ul style="list-style-type: none"> No additional actions planned 	

Risk/Threat	Risk Rankings		Control Evaluation – March 2016	Management Strategy for risk and IA
16. HelpDesk survey response rate does not allow for effective measurement	Tolerance: High	Impact: Minor	Current Controls: A survey is sent with every ticket that is closed.	Evaluate the anticipated risk levels
	Controls: Some Vulnerability	Likelihood: Some Likelihood	Future Actions: TSD will review survey procedures with SPAT.	
17. Unplanned hardware/software/licensing purchases adversely impact pre-planned purchases	Tolerance: Low	Impact: Minor	Current Controls: HelpDesk purchase requests are reviewed and prioritized by NIS management as they are submitted. Purchase requests must first be approved by the requestor’s supervisor. SMT is involved once a dollar threshold is reached. Unplanned purchases are subject to budget availability.	Accept the anticipated risk levels
	Controls: Strong	Likelihood: Some Likelihood	Future Actions: ○ No additional actions planned	
18. ASRS software licensing compliance is not adequate	Tolerance: Low	Impact: Moderate	Current Controls: A software asset licensing tool records the licenses as they are purchased. Twice per year reconciliations of installations to purchases are performed. Some agreements involve semi-annual true-ups (at six month mark buy any additional licensing as needed). Manual checks are performed against what is installed to determine license availability at the time of request for certain software. Internal Audit conducts periodic reviews.	Reduce the anticipated risk levels
	Controls: Some Vulnerability	Likelihood: Some Likelihood	Future Actions: Management is enhancing the tool and/or process to ensure ASRS maintains compliance (regular discoveries, etc.).	

Risk/Threat	Risk Rankings		Control Evaluation – March 2016	Management Strategy for risk and IA
19. Vendor licensing structures are too complex to effectively manage	Tolerance: Medium	Impact: Moderate	Current Controls: Detailed contract reviews are conducted by TSD and Procurement prior to purchase or upon ownership or product changes. NIS consults with Procurement when contract licensing questions arise.	Accept the anticipated risk levels
	Controls: Some Vulnerability	Likelihood: Some Likelihood	Future Actions: No additional actions planned.	
20. End User Licensing Agreements (EULAs) are being accepted by unqualified staff resulting in undesirable terms and conditions	Tolerance: High	Impact: Moderate	Current Controls: Procurement and TSD staff review licensing agreements and EULAs (if available) at the time of purchase.	Evaluate the anticipated risk levels
	Controls: Weak	Likelihood: Some Likelihood	Future Actions: <ul style="list-style-type: none"> • Management is evaluating • TSD will follow-up with SMT in six months (approx. Sept-Oct 2016) 	
21. Lack of autonomy to make technology investments to meet business needs	Tolerance: Medium	Impact: Moderate	Current Controls: The agency has aligned itself with the checks and balances put in place by ADOA. Strong relationships are established with ASET, OSPB and JLBC.	Accept the anticipated risk levels
	Controls: Some Vulnerability	Likelihood: Some Likelihood	Future Actions: No additional actions planned	

Risk/Threat	Risk Rankings		Control Evaluation – March 2016	Management Strategy for risk and IA
22. FTEs are not fully trained in all areas of responsibility	Tolerance: Medium	Impact: Moderate	<p>Current Controls: Operations geared toward meeting clearly defined NIST standards, overseen and supported by ERM. New hires are generally hired for their technical skills but additional on the job training is required for tools, technologies and processes before they can be fully productive (3 to 9 months). Cross-training has been increased for all networking activities. Other TSD resources are used to fill gaps in knowledge. Professional services are available for specialized projects (includes on-going support in some cases).</p>	Reduce the anticipated risk levels
	Controls: Some Vulnerability	Likelihood: Some Likelihood	<p>Future Actions:</p> <ul style="list-style-type: none"> • Management should consider: <ul style="list-style-type: none"> ○ More advanced training in various technical areas (i.e. virtualization, multiple operating systems, and project management methodologies) ○ Purchasing training when a new hardware and/or software is purchased 	
23. TSD is not involved early enough in business-led, non-TSD managed projects to properly assess technology impact	Tolerance: Medium	Impact: Minor	<p>Current Controls: Some business-led projects have TSD representatives on their steering committees. Only TSD purchases software. A process is in place to include TSD while considering cloud endeavors. TSD communicates to SMT when competing priorities exist.</p>	Evaluate the anticipated risk levels

Risk/Threat	Risk Rankings		Control Evaluation – March 2016	Management Strategy for risk and IA
	Controls: Some Vulnerability	Likelihood: Some Likelihood	Future Actions: Management should consider following a standard process for non-TSD led projects to ensure technology needs are considered early enough to provide adequate lead time.	
24. A system breach goes undetected for a period of time	Tolerance: Low	Impact: Major	Current Controls: Operations geared toward meeting clearly defined NIST standards, overseen and supported by ERMC. Forensic data capture is in place including back-ups, system logging, and database audit vault. Notifications of vulnerabilities are received from external and internal entities. Resources are redirected to address threats. Industry standard devices and practices are utilized within ASRS IT environment. Processes and procedures are in place to remediate vulnerabilities. Automatic updating of threat definitions on various security appliances. Cyber risk insurance is in place.	Reduce the anticipated risk levels
	Controls: Some Vulnerability	Likelihood: Some Likelihood	Future Actions: <ul style="list-style-type: none"> • Achieve targeted Gartner Security Maturity levels. • Additional measures will be implemented under the 5 year plan • Recruitment is underway for additional security resources 	

Risk/Threat	Risk Rankings		Control Evaluation – March 2016	Management Strategy for risk and IA
25. Data is stored in the cloud without approval	Tolerance: Medium	Impact: Minor	<p>Current Controls: Operations geared toward meeting clearly defined NIST standards, overseen and supported by ERMC. A cloud policy and SOP are in place and have been communicated. SMT must approve new and modifications to existing cloud ventures. A security questionnaire for each vendor and venture is sent as described in the cloud policy.</p>	<p>Evaluate the anticipated risk levels</p> <p>IA should review technology usage to ensure participation in the cloud is as approved</p>
	Controls: Some Vulnerability	Likelihood: Likely	<p>Future Actions:</p> <ul style="list-style-type: none"> • TSD will collaborate with external entities (i.e. ADOA, ISO meetings, etc.) to determine if ASRS should modify current practices related to cloud endeavors. • Management should consider: <ul style="list-style-type: none"> ○ Options to review cloud policy compliance. ○ Having IA review technology usage to ensure participation in the cloud is as approved 	

Continuity of Operations Plan (COOP)

Risk/Threat	Risk Rankings		Control Evaluation – March 2016	Management Strategy for risk and IA
<p>1. Business continuity plans are not established, tested, reviewed or sufficient to support business operations in the event of a disaster.</p>	<p>Tolerance: Low</p>	<p>Impact: Major</p>	<p>Current Controls: Periodic comprehensive tests are performed to evaluate the ability to recover core business systems at our alternate site should a short duration incident occur. IMD’s COOP is integrated into overall agency COOP. The Business Impact Assessment (BIA) is periodically reviewed and updated to verify threats, recovery time objectives, and disaster recovery (DR) staffing requirements. Internal Audit monitors COOP tests and consults as necessary. COOP plan is housed with Department of Emergency and Military Affairs (DEMA).</p>	<p>Accept the anticipated risk levels</p>
	<p>Controls: Strong</p>	<p>Likelihood: Not Likely</p>	<p>Future Actions:</p> <ul style="list-style-type: none"> • A COOP update is underway 	

Risk/Threat	Risk Rankings		Control Evaluation – March 2016	Management Strategy for risk and IA
<p>2. Current COOP infrastructure in the alternate site is inadequate to support business needs in the event of a short-term emergency</p>	<p>Tolerance: Medium</p>	<p>Impact: Minor</p>	<p>Current Controls: The after-action reports are considered when evaluating equipment purchases for the alternate site. COOP exercise results are utilized to enhance system performance. The current process is to limit the number of persons utilizing the systems and the order in which work is performed to bring up infrastructure. Regular reviews are performed to determine the business impact of each system to prioritize adequacy. Each division has identified critical systems that must be operational within designated timeframes in a disaster situation and management is aware of current infrastructure limitations. Each division has assigned appropriate personnel to their role in a disaster. A procedure is in place to work with Procurement to acquire any essential equipment during a disaster. Additional equipment has been purchased and implemented at the alternate site. Periodic reviews are conducted to determine needs to modernize equipment.</p>	<p>Evaluate the anticipated risk levels</p>
	<p>Controls: Some Vulnerability</p>	<p>Likelihood: Some Likelihood</p>	<p>Future Actions: Management should consider capability at the alternate site to ensure requirements have not changed.</p>	

Risk/Threat	Risk Rankings		Control Evaluation – March 2016	Management Strategy for risk and IA
3. Emergency communications are not executed effectively	Tolerance: Low	Impact: Moderate	<p>Current Controls: An emergency contact phone tree is regularly updated. Text messaging and email groups have been established for the Crisis Management Team. A conference line is in place that can be used in an emergency situation. Staff is aware of their COOP role (telecommute, drive to alternate site, administrative leave, etc.). An SOP is in place. Communication is discussed during the COOP exercises, whether live or tabletop. TSD works cooperatively with DEMA.</p>	Reduce the anticipated risk levels
	Controls: Some Vulnerability	Likelihood: Some Likelihood	Future Actions: Management should consider more frequent tests of the communicator system.	
4. COOP infrastructure in the alternate site is unavailable at the same time the primary site is unavailable	Tolerance: High	Impact: Major	<p>Current Controls: The alternate site is more than 100 miles from the primary site to reduce the likelihood of risk occurrence. Upon request the disbursement bank can issue payrolls based on previous month's pension run. The public ASRS website is hosted offsite. IMD has provisions to continue operations independent of the alternate site.</p>	Accept the anticipated risk levels
	Controls: Weak	Likelihood: Not Likely	Future Actions: No additional actions planned	

Agenda Item #5B



ARIZONA STATE RETIREMENT SYSTEM

3300 NORTH CENTRAL AVENUE • PO BOX 33910 • PHOENIX, AZ 85067-3910 • PHONE (602) 240-2000
4400 EAST BROADWAY BOULEVARD • SUITE 200 • TUCSON, AZ 85711-3554 • PHONE (520) 239-3100
TOLL FREE OUTSIDE METRO PHOENIX AND TUCSON 1 (800) 621-3778

Paul Matson
Director

MEMORANDUM

TO: Mr. Jeff Tyne, Chair, Operations and Audit Committee (OAC)

FROM: Mr. Anthony Guarino, Deputy Director and Chief Operations Officer
Mr. Kent Smith, Assistant Director, Technology Services Division (TSD)
Mr. Thomas Keown, Information Security Officer, TSD
Ms. Molly Mahai, Manager, Network Information Systems, TSD

DATE: March 31, 2016

RE: **Agenda Item #5.B.:** Presentation, Discussion and Appropriate Regarding the ASRS External Information Technology (IT) Security Audit

Purpose

To discuss the results of the 2016 IT Security Posture Assessment and Penetration Testing.

Recommendation

Informational only, no action required.

External Security Audit

An external security audit was conducted during the week of January 18, by RiskSense (formerly CAaNES). The scope of this audit included the following:

- internal and external penetration,
- vulnerability scanning,
- social engineering phishing email attempts,
- security compliance review.

The ASRS has standardized on the National Institute of Standards and Technology (NIST) controls, which are recommended by the state's CIO. RiskSense used these controls to measure our security posture and the maturity of our security program.

The results of this year's assessment will be discussed in Executive Session at the April 12, 2016 meeting.

Enclosed you will find the following confidential materials:

- A. Arizona State Retirement System Security Assessment presentation from RiskSense
- B. ASRS Response to Security Assessment 2016

**Confidential materials
were provided to the
Trustees and not
included in this book.**