ICSA – Information Technology (due April 30, 2024)

Each agency is responsible for establishing and maintaining an effective system of internal control. Internal controls can provide reasonable, but not absolute, assurance that an agency's objectives—including the prevention or detection of fraud, waste and abuse—will be met. More information about internal controls and minimal internal control structure requirements can be found in Topic 05 of the State of Arizona Accounting Manual (SAAM). The internal control self-assessment is meant as a catalyst to improve agency operations and achieve agency objectives.

This survey is a self-assessment of certain internal control practices within your agency in the area of Information Technology. Some of these practices may not be required by policy but are nonetheless considered best practices.

If your response to a survey item is sensitive in nature, contact GAO's Internal Audit Unit (gaointernalaudit@azdoa.gov, 602-291-0506) directly to discuss.

The items in this survey are to be rated, using either Yes/No/NA or the 5-point scale as indicated by each question. The following guidance is provided for the 5-point scale ratings:

Not Applicable (0) – Practice does not apply.

Needs Improvement (1) – Practices have not been fully implemented or are intermittent; acceptable quality and timeliness are recurring challenges.

Fair (2) – Practices meet the minimum expectations but are not consistently monitored; acceptable quality and timeliness are inconsistent.

Good (3) – Practices meet expectations and are monitored frequently; acceptable quality and timeliness are consistent.

Very Good (4) – Practices exceed expectations; quality and timeliness are consistently above average.

Excellent (5) – Practices serve as a model for other agencies and other states; quality and timeliness exceed expectations; best-in-class results.

ICSA – Information Technology (due April 30, 2024)

EMAIL:
Agency Name:
Contact Name (First and Last):
Contact Number (Work Phone):
EIN:
CFO/CFO Designee Email Address:

Information Technology

Internal controls over information technology help maintain the integrity and security of system data. The survey items below are driven by SAAM policies, Arizona Strategic Enterprise Technology (ASET), ASET policies, and best practices. For more information on ASET policies and best practices, visit the ASET website at: https://aset.az.gov/ for general information and https://aset.az.gov/policies-standards-and-procedures and https://azdohs.gov/information-technology-it-policies-standards-and-procedures for policies and procedures. The survey items below are intended for IT network and/or software applications maintained at the State level (e.g., AFIS/AZ360, APP, HRIS) and the agency level (e.g., purchased or internally developed).

1. Agency accepts payment cards (Y/N). If N, skip to #2.
   1a. Agency conducts annual PCI IT Risk Assessment as required by SAAM 4018. (1-5 scale)
   1b. Agency conducts annual PCI Non-IT Risk Matrix as required by SAAM 4018. (1-5 scale)
2. Adequate physical security measures exist over access to servers, storage media, computers, ports and terminals. (1-5 scale) (IT: Physical Security Protections Policy P8260.)
3. Employee access to statewide systems and software applications is promptly updated for any change in user roles, transfers or terminations. (1-5 scale) (SAAM 0507 and IT: Identification and Authentication Policy P8340.)
4. Logical access to statewide systems and software applications is limited to authorized employees. (1-5 scale) (SAAM 0540 and IT: Identification and Authentication Policy P8340.)
5. Agency maintains IT network or software applications at the agency level. (Y/N) (If N, submit survey).
6. Please describe any computerized systems and software applications maintained at the agency level related to accounting (not AFIS/AZ360). This would include, but is not limited to, any system related to billing, receipts, licensing, purchasing, P-Cards, invoice processing, disbursements, fixed assets, inventory, point-of-sale, travel, and grants. (Comments Box Only).
   6a. Are your financial systems reconciled to AFIS/AZ360 at least on a monthly basis? (0-5 scale)

7. Computerized systems and application software are secured through the use of passwords. (1-5 scale) (IT: Acceptable Use Policy P8280 and Identification and Authentication Policy P8340.)
8. Each user has their own individual password. Sharing passwords is prohibited. (1-5 scale) (SAAM 0507 and IT: Acceptable Use Policy P8280 and Identification and Authentication Policy P8340.)
9. Passwords are required to be changed at least on a quarterly basis. (1-5 scale) (IT: Identification and Authentication Standard S8340.)
10. Data backup and recovery procedures are established, maintained and followed for all applications. (1-5 scale) (IT: Contingency Planning Policy P8230 and Incident Response Planning Policy P8240/)
    Agency practices are consistently followed to ensure:
    10a. Agency practices are consistently followed to ensure: Frequent backup of data files. (0-5 scale)
    10b. Agency practices are consistently followed to ensure: Secured off-site storage of all backup data files and programs. (0-5 scale)
    10c. Agency practices are consistently followed to ensure: Recovery procedures are tested at least annually with documentation of results. (0-5 scale)
11. System documentation is readily accessible either electronically or in hard copy, including descriptions of hardware and software, operator manuals, etc. (1-5 scale)
12. Security logs are generated by the system. (Yes/No) (IT: System Security Audit Policy P8330.) (If No, skip to 13.)
    12a. Security logs are routinely reviewed for evidence of multiple unsuccessful attempts to log-on. (1-5 scale) (IT: System Security Audit Policy P8330.)
13. The system denies user access after a maximum of six consecutive invalid log-on attempts. (1-5 scale) (IT: Access Control Standard S8320.)
14. All employees, contractors, and volunteers with access to State systems are required to take an annual cybersecurity training. (1-5 scale)

Comments:
Add comments/clarity for all questions where your agency has selected NA. You may add additional comments as necessary.