Arizona Department of Agriculture

Department did not comply with all statutory conflict-of-interest requirements and effectively safeguard its IT systems and sensitive data

Audit purpose

To determine whether the Department complied with statutory conflict-of-interest requirements and information technology (IT) security requirements and best practices; and provide responses to the statutory sunset factors.

Key findings

- Department did not comply with several statutory conflict-of-interest requirements and best practices, such as ensuring that all council/committee members complete conflict-of-interest disclosure forms, requiring employees and council/committee members to complete or update disclosure forms annually, or maintaining the statutorily required special disclosure file.
- Noncompliance with statutory and Department conflict-of-interest requirements, as well as best practices, increased the risk of employees and council/committee members not disclosing substantial interests.
- Department did not perform key IT security requirements, including conducting an annual IT security risk assessment of its IT systems, incorporating IT security requirements into its web application development, managing its web application accounts to ensure only appropriate and authorized access to its applications, and ensuring vulnerability scanning of its IT systems was consistently performed.
- Department has not established an adequate IT security governance structure to help ensure that its IT systems and sensitive data are adequately safeguarded.
- Department-supported councils and committees did not always comply with various provisions of the State's open meeting laws.

Key recommendations

The Department should:

- Comply with statutory conflict-of-interest requirements and best practices.
- Update and implement its policies and procedures to comply with the State's conflict-of-interest requirements and best practices.
- Conduct an annual risk assessment of its IT systems, incorporate security requirements into its web application development, appropriately manage web application accounts, and continue to ensure that vulnerability scans of its IT systems are performed.
- Develop and implement an IT security governance framework.
- Ensure that the various councils and committees it supports comply with all State open meeting law provisions.