Why This Assessment Is Important

Information Technology (IT) plays an essential role in business operations by collecting, processing, and housing business data. Identifying IT risks and establishing sound internal controls can help mitigate negative events, including hardware and software failure, human error, scams and phishing, viruses and malicious attacks, and security breaches.

Our IT Risk Assessment Refresh included:

1. Conducting a countywide IT survey to identify key software applications used by county departments, and to better understand current IT risks related to IT applications, initiatives, processes, and data sensitivity within each department.

2. Updating the status of the Office of Enterprise Technology (OET)'s cybersecurity assessment goals identified in our prior 2016 report.

The information collected during our review was self-reported by the departments and was not verified or audited. The risk assessment results are used by Internal Audit to prioritize future IT internal audits and related resource planning.

Risk Assessment

Following is a summary of work performed. We have reviewed this information with OET management and appreciate the excellent cooperation provided by management and staff.

Key Software Applications

We sent a questionnaire to county departments requesting information regarding key applications and controls used in performing their business operations. We had a 100% response rate. Questionnaire responses identified over 630 applications used by departments throughout the County. The questionnaire focused on the following key application risk areas:
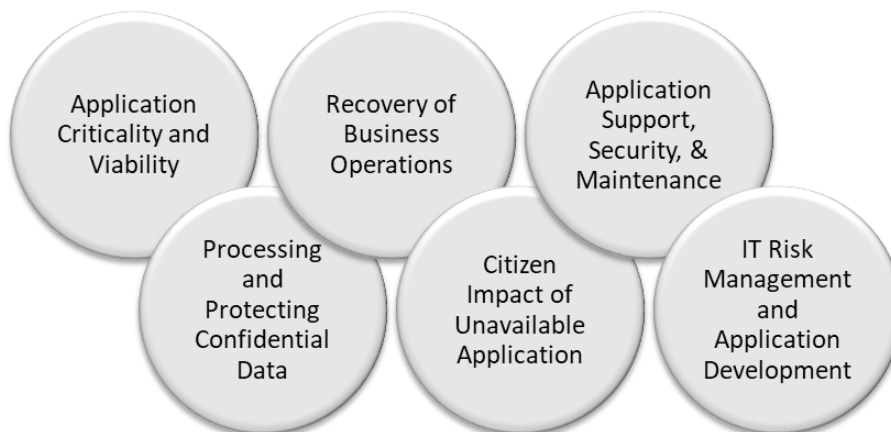
For security purposes, survey result details and our assessments are restricted from this report. However, nothing came to our attention that warrants the Board's consideration. Survey result details were discussed and shared with OET to help improve security and network support.

Cybersecurity

We performed a cybersecurity assessment in 2016 using a third-party evaluator. We assessed OET's cybersecurity maturity for 10 key risk areas and assigned a maturity rating. In addition, OET identified its desired maturity for each area and developed goals to reach the desired state.

Through interviews with OET's InfoSec Division management, we documented OET's progress in implementing the established goals from 2016. Of the 10 key cybersecurity risk areas considered, OET reported making meaningful progress in seven areas. OET reevaluated some previously planned approaches due to changes in the risk environment and availability of new technology solutions. This resulted in adjustments to some of the roadmaps and delayed progress on others.

Overall, we found that OET's InfoSec Division is making satisfactory progress toward accomplishing its established goals. For security purposes, assessment details are restricted from this report. However, nothing came to our attention that warrants the Board's consideration.

Additional Information

This assessment was approved by the Maricopa County Board of Supervisors and was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing. This report is intended primarily for Maricopa County Board of Supervisors. However, this report is a public record, and its distribution is not limited. If you have any questions about this report, please contact Mike McGee, Internal Audit Director, at 602-506-1585.