



# Maricopa County

Internal Audit Department

301 West Jefferson Street  
Suite 660  
Phoenix, AZ 85003-2148  
Phone: 602-506-1585  
Fax: 602-506-8957  
www.maricopa.gov

**To:** Andrew Kunasek, Chairman, Board of Supervisors  
Fulton Brock, Supervisor, District I  
Don Stapley, Supervisor, District II  
Max W. Wilson, Supervisor, District IV  
Mary Rose Wilcox, Supervisor, District V

**From:** Ross L. Tate, County Auditor 

**Subject:** Countywide IT Inventory: Risk Identification

**Date:** February 16, 2011

---

## Executive Summary

We completed the Countywide IT Inventory in accordance with our Board-approved audit plan. The scope of our review included obtaining IT surveys from several County agencies<sup>1</sup> and conducting interviews with selected agencies based on survey responses. Our objective was to identify significant County IT risks by conducting an agency self-reported IT inventory of key agency applications, systems, initiatives, and data sensitivity. This report identifies the top three Countywide IT risks (listed below). Internal Audit will use the information obtained during this review for future audit planning. The consulting firm of KPMG LLP assisted us in this engagement.

### Countywide IT Risks

- Inadequate data privacy controls could result in lost or stolen data.
- Weak IT governance processes could result in IT plans that do not align with the County's overall strategic plan leading to uncontrolled expenditures and/or subpar systems.
- Aging IT systems relied upon by users for key business processes may not perform efficiently.

---

<sup>1</sup> See Appendix A for a list of agencies.

## Background

The IT Risk Assessment, conducted by Internal Audit in 2004, noted that most County risks were associated with network security and data center assets, such as disaster recovery/business continuity planning, network and wireless (Wi-Fi) security, and computer virus protection. Recent interviews with the County’s Office of Enterprise Technology (OET) and other agencies show that the County has addressed network availability and security risks by implementing the following:

- Network zoning – Uses segregating devices connected to the network to enable computer equipment to run more efficiently. Breaking up a network into zones distributes activity so no single device is overwhelmed. Zoning also improves data integrity and enhances security by restricting access to certain areas within the network based on need. For example, law enforcement information is restricted to its own zone and only employees with clearance are given access rights.
- Commercial disaster recovery service or “hot site” – Allows the County to continue computer and network operations in the event of a disaster.

Not all agencies have documented disaster recovery plans, so disaster recovery continues to be a focus. However, network-related risks appear to have lessened when compared to data-related risks. The County, like other governments and corporations, has shifted from a network-focused to a data-focused environment. Data is no longer contained within an organization’s network. Critical data has been extended from the network to the laptop, BlackBerry, USB drive, and third-party service providers who host data and applications on the Internet. Protecting data begins with adequately implementing data security solutions.

The County requires skilled IT professionals to effectively oversee its mission-critical systems and data storage/management. Currently, the County has 480 full-time IT employee positions<sup>2</sup>. The following table compares this number to the 2009 U.S. national average. While the county is close to the national average, several IT positions are currently vacant as agencies search for viable candidates or work leaner due to the current economic environment.

**Full-Time IT Employees as a Percentage of Total Employees**

Total IT Employees	Total Employees Countywide	IT Employees as % of Total Employees
480	13,526	3.55%
Avg. % U.S. Local Gov. IT Employees as a % Total Employees <sup>3</sup>		3.80%

<sup>2</sup> See Appendix B for total number of full-time IT employees by agency.

<sup>3</sup> Sacramento County, *Comparison of IT Spending, Staffing, and Services in Counties Similar to Sacramento County*, May 26, 2010:

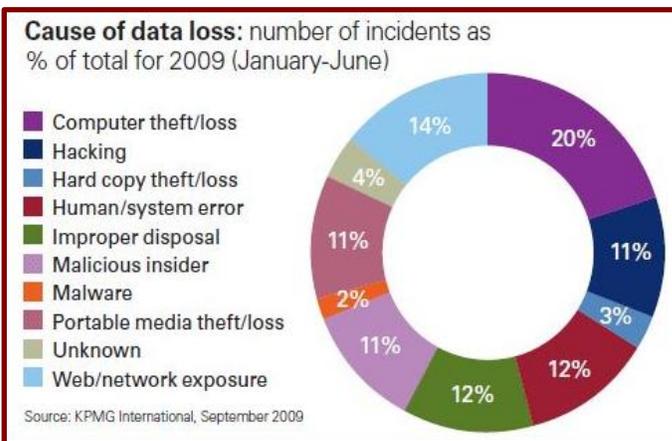
[http://www.ocit.saccounty.net/coswcm/groups/public/@wcm/@pub/@ocit/@inter/documents/webcontent/sac\\_024082.pdf](http://www.ocit.saccounty.net/coswcm/groups/public/@wcm/@pub/@ocit/@inter/documents/webcontent/sac_024082.pdf)

## Maricopa County's Top IT Risks

Data privacy, IT Governance, and legacy (older, aging) enterprise applications appear to be the County's top three IT risks.

### 1. Data Privacy

As technology and the Internet have made it easier to collect personal information for legitimate business purposes, criminal exploitation of sensitive information is also on the rise. The challenge is to share data while protecting personal information. Various statutes and regulations<sup>4</sup> require organizations to protect collected and stored sensitive personal data. Data privacy policies are essential for effective data information security.



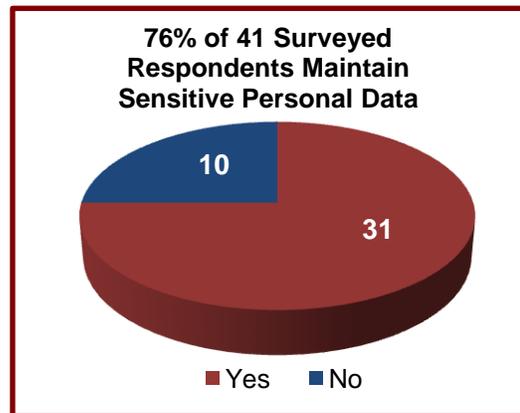
Sources of Data Loss Worldwide

Worldwide, from 2005 to 2009, there were more than 2,300 publicly disclosed data breaches impacting 700 million people. Since many are unreported, this may be the tip of the iceberg.<sup>5</sup> The KPMG Data Loss Barometer at left shows that the leading cause of data breaches in 2009 was from lost or stolen laptops. When combined with other portable media (USB drives and mobile devices), nearly a third of all data breaches resulted from lost or stolen portable devices.

Seventy-six percent of our IT inventory survey respondents stated their agency collects and maintains sensitive information. This information ranged from general personally identifiable information (PII) such as name, address, phone number, date of birth, and social security numbers, to highly confidential PII such as medical records and law enforcement data.<sup>6</sup>

According to a County Risk Management report on computer loss claims, 48 County computers were lost or stolen between 2005 and 2010.

Risk Management states that this list may be incomplete, as some agencies do not seek insurance reimbursement for replacement and may not report missing items. OET reports that laptop encryption for the 30 agencies it supports is under way.



<sup>4</sup> Examples: Arizona Security Breach Law ARS 44-7501, The Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry Compliance Data Security Standards (PCI DSS).

<sup>5</sup> KPMG International, *Data Loss Barometer*, [www.datalossbarometer.com](http://www.datalossbarometer.com).

<sup>6</sup> See Appendix C for more detailed information on types of personal information collected at the County.

We informally compared the County's current data privacy controls with several other local governments. Both the City of Phoenix and the State of Arizona report that they have implemented policies for handling various classes of personally identifiable information. See Appendix C for additional information relating to personally identifiable information maintained within County agencies.

### **County Data Privacy Controls are Weak**

While the County maintains many types of personal and sensitive data, self-reported surveys and agency follow-up interviews show that the County has not:

- Implemented a formalized privacy program.
- Installed laptop encryption to minimize the risk of data breaches resulting from lost or stolen laptops.
- Implemented a robust asset management system to identify and track lost or stolen laptops.
- Installed data loss prevention technologies to identify and detect potential data privacy risks and violations.

Proper data security not only protects the data but also the business. Non-existent or insufficient data privacy programs could result in data breaches through insider theft, external hacking, or physical theft. Breaches may result in hard costs to remediate the breach, including notification, credit monitoring, remunerations, and fines and penalties for regulatory non-compliance. Breaches may also result in a tarnished reputation. The Ponemon Institute, an independent research agency, reported that the 2009 average cost for U.S. organizations of a data-loss incident was \$6.75 million, or \$204 per compromised record.<sup>7</sup>

Effective enterprise-wide privacy programs (1) focus on data loss prevention, including identifying and responding to data breaches and (2) include business process and IT-based controls that are consistent with the organization's overall privacy requirements.

## **2. IT Governance**

IT governance is the term for how management formally decides to employ IT in supervising, monitoring, and directing the organization. Effective IT governance ensures that IT performance creates real value, manages IT-related risks, and optimizes resources. If the decision-making process is not formalized, IT governance is deemed less than optimal. The MIT Sloan School of Management Center for Information System Research found that private firms with superior IT governance generate 40 percent higher returns on investment (ROI)<sup>8</sup>.

---

<sup>7</sup>SC Magazine, *U.S. Organizations Face the Highest Data Breach Costs*, Angela Moscaritolo, 30 Apr 2010  
<http://www.scmagazineus.com/us-organizations-face-the-highest-data-breach-costs/article/169160/>

<sup>8</sup>Shayne Kavanagh and David Melbye, *Shrewd Investing in IT Assets through IT Governance*, Government Finance Review, February 2009, published by Government Finance Officers Associations (GFOA).

Effective governance requires the Chief Information Officer (CIO) to collaborate with an organization's executive business leaders. When key stakeholders do not actively create, approve, prioritize, and execute IT-related plans in concert with the CIO, the risk of IT failures increase. Extensive business knowledge, not just technology expertise must be used to guide IT decisions.<sup>9</sup>

### Why is IT Governance Important?

IT spending can rise quickly as technology embeds itself in every business process. IT investments include hardware, software, maintenance, human resources (adequate staffing, training, and retention), and security. To help maximize IT value and minimize risk, an organization should involve organization-wide stakeholders in decision-making and accountability. IT governance can increase the likelihood of positive, effective, cost-beneficial outcomes, and help entities achieve their desired benefits.

**“There is no silver-bullet technology that fits any budget and unfailingly pays back the investment. The key to getting value from technology investments is IT governance.”**  
**GFOA<sup>10</sup>**

### Maricopa County IT Governance Can Be Enhanced

The current status of the County's IT governance program continues to be a significant IT risk. During our review, we found that Maricopa County's current IT governance has outdated and incomplete IT governance policies. This risk was previously identified in our June 11, 2009 report<sup>11</sup> entitled, “Countywide Information Technology (IT) Governance Review.” OET reports that it is working toward submitting an IT Governance policy to the Board for approval.

OET is developing an enterprise-wide IT governance committee that will include representation from all agencies and elected officials. Internal Audit supports this plan and encourages agency leadership to carefully collaborate with IT leadership in developing a sound IT governance program that establishes IT governance policies and implements best practices.

Effective IT governance can save millions of dollars and ensure that IT solutions successfully meet critical business needs and customer services. Ineffective IT governance can result in costly failed IT projects and poor IT investments. Without a strong IT governance program, IT plans may not align with the County's overall strategic plan. An ineffective IT governance program could also lead to unimplemented decisions, incomplete information,

---

<sup>9</sup> *IT Governance and Business Outcomes - A Shared Responsibility between IT and Business Leadership*, NASCIO Governance Series, March 2008, published by National Association of State CIOs (NASCIO) <http://www.nascio.org/publications/documents/NASCIO-ITGovernanceBusinessOutcomes.pdf>.

<sup>10</sup> Shayne Kavanagh and David Melbye, *Shrewd Investing in IT Assets through IT Governance*, *Government Finance Review*, February 2009, published by Government Finance Officers Associations (GFOA).

<sup>11</sup> Maricopa County Internal Audit, *Countywide Information Technology (IT) Governance Review*, [www.maricopa.gov/Internal\\_audit/PubDocuments/FY2009/ITGovReport.pdf](http://www.maricopa.gov/Internal_audit/PubDocuments/FY2009/ITGovReport.pdf)

inaccurate cost estimates, uncontrolled expenditures, ineffective systems, incomplete performance measures, and noncompliance with laws and/or regulations.

### **3. Legacy Systems**

A “legacy system” is any older application program that remains in use even though there are newer and more streamlined computer technologies and applications available. Sound IT controls include regularly assessing the capability and performance of legacy systems. System performance is defined as the contribution the system makes to business objectives, functionality, stability, complexity, costs, strengths and weaknesses.<sup>12</sup> See Appendix D for additional information relating to County IT applications.

#### **Maricopa County Enterprise Legacy Applications**

The County has several older applications that will probably soon require updating. Examples of the most critical applications requiring updates include the Financial System (Advantage), portions of the Treasurer’s System, and the Jail Management System.

Each of these applications is nearly 20 years old and the underlying technology is becoming more difficult and costly to support. As an example, all agencies use Advantage; however, the number of knowledgeable and experienced support personnel has significantly declined due to staff departures and the outsourcing of application maintenance. Newer accounting packages offer customized management reports that help business owners review financial and operational information to make informed decisions.

The County’s legacy enterprise financial information system meets day-to-day operational requirements; however, it does not provide the robust business analytic capabilities necessary to make better informed management decisions. The County has made available to agencies a separate analytical and business reporting software application that can be used to analyze budget and accounting transactions. This additional application assists management in gathering the timely and accurate financial information they need to make informed decisions.

As County management evaluates upgrade solutions and identifies the resources needed to effectively implement a new system, it will also need to allocate internal resources to maintain day-to-day operations. However, the County should not begin upgrading or replacing its existing enterprise financial systems without first implementing an effective enterprise-wide IT governance infrastructure.

As an example, Florida suspended work on a 3-year, \$100 million IT project, declaring it an expensive failure. Florida hired a private firm for \$89 million to develop a streamlined accounting system, but ended up using its 25-year-old system. Gartner Group<sup>13</sup> concluded that the Florida IT project failed due to a lack of IT governance.<sup>14</sup> The Florida example

---

<sup>12</sup> See COBIT Objective 1.3 Assessment of Current Capability and Performance. The Control Objectives for Information and related Technology (COBIT) is a set of best practices (framework) for information technology (IT) management created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI).

<sup>13</sup> Gartner Group is a well-recognized information technology research and advisory company.

<sup>14</sup> Steve Bousquet, *\$89M Down the State Drain* (May 18, 2007)

shows that failure to implement an effective Countywide IT governance approach significantly increases the likelihood of a failed implementation.

We reviewed this report with OET management. We would like to thank each of the agencies that participated in the surveys and interviews, especially the Office of Enterprise Technology, Assessor's Office, Human Services Department, and Integrated Criminal Justice Information System (ICJIS) for their assistance with piloting the IT Inventory survey. If you have any questions or wish to discuss the information presented in this memo, please contact me at (602) 506-1585 or Eve Murillo at (602) 506-7245.

C: David Smith, County Manager  
Sandi Wilson, Deputy County Manager  
Stephen Wetzel, Chief Information Officer, Office of Enterprise Technology

## APPENDIX A

### IT Inventory Participating Agencies\*

Agency	IT Survey	Follow-up Interviews**
Adult Probation	✓	
Air Quality	✓	✓
Animal Care and Control	✓	
Assessor	✓	
Clerk of the Superior Court	✓	✓
Correctional Health	✓	✓
County Attorney	✓	
Education Services	✓	
Emergency Management	✓	
Environmental Services	✓	✓
Equipment Services	✓	
Facilities Management	✓	
Finance	✓	✓
Flood Control	✓	
Human Resources	✓	✓
Human Services	✓	
ICJIS	✓	
Justice Courts	✓	
Juvenile Defender	✓	
Juvenile Probation	✓	
Legal Advocate	✓	
Legal Defender	✓	
Library District	✓	
Materials Management	✓	✓
Medical Examiner	✓	
Office of Enterprise Technology (OET)	✓	✓
Office of Management and Budget	✓	
Parks and Recreation	✓	
Planning and Development	✓	✓
Public Defender	✓	
Public Health	✓	✓
Recorder	✓	
Risk Management	✓	✓
Solid Waste	✓	
Special Litigation	✓	
STAR Call Center	✓	
Superior Court	✓	✓
Transportation	✓	✓
Treasurer	✓	✓

\* RDSA and Public Works also provided enterprise-wide survey responses.

\*\* Internal Audit conducted follow-up interviews based on auditor review of agency survey responses.

## APPENDIX B

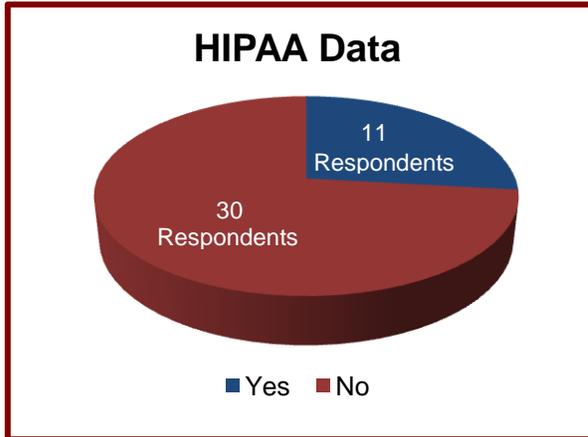
### Total Number of Full-Time IT Employees by Agency <sup>15</sup>

Agency	# of IT FTEs
Office of Enterprise Technology	97
Superior Court	75
Sheriff's Office	58
Public Works	47
Clerk of the Superior Court	37
County Attorney	31
Assessor	28
Recorder	26
Planning and Development	21
Public Defense System	11
Treasurer	11
Adult Probation	8
Human Services	6
County Manager	4
Elections	4
Juvenile Probation	3
Public Health	3
Education Services	2
Correctional Health	2
Materials Management	2
Animal Care and Control	1
Justice Courts	1
STAR Call Center	1
Workforce Management and Development	1
<b>TOTAL IT EMPLOYEES</b>	<b>480</b>

<sup>15</sup> Obtained from Maricopa County FY 2010–11 Annual Business Strategies Recommended Budget

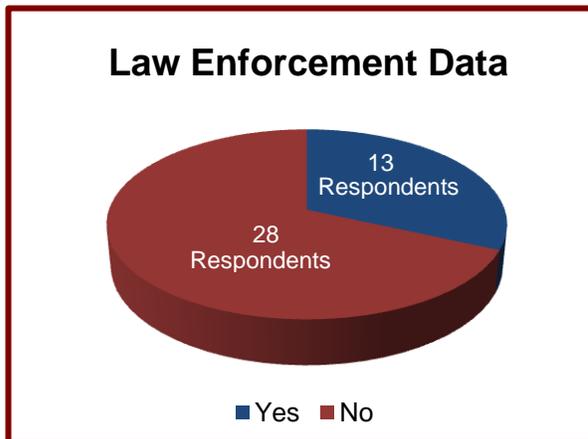
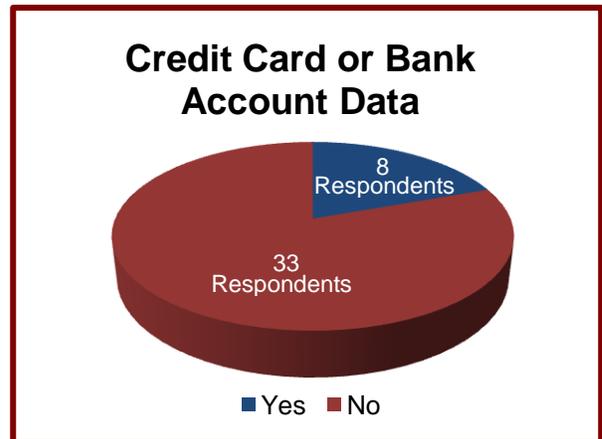
## APPENDIX C<sup>16</sup>

### Personally Identifiable Information



27% of responding agencies report collecting and maintaining Health Insurance Portability and Accountability Act (HIPAA) data.

20% of responding agencies report collecting and maintaining credit card or bank account data.



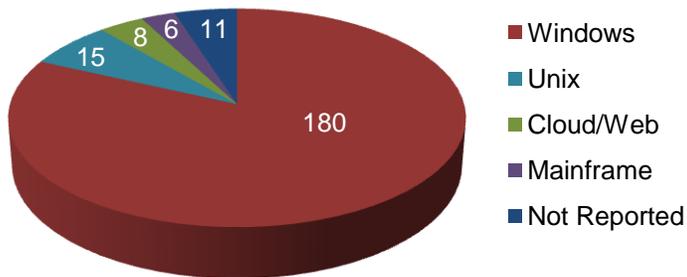
32% of responding agencies report collecting and maintaining law enforcement data.

<sup>16</sup> All data in Appendices C and D was provided from agency survey responses.

## APPENDIX D

### Other IT Inventory Application Information

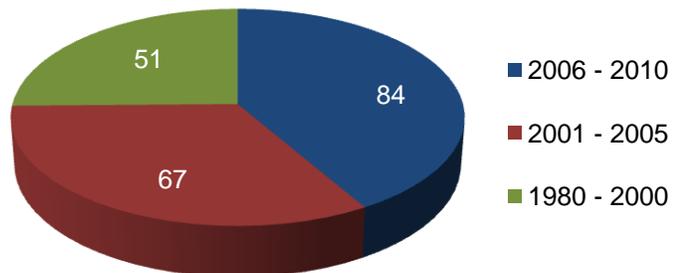
#### Operating Systems and Architecture



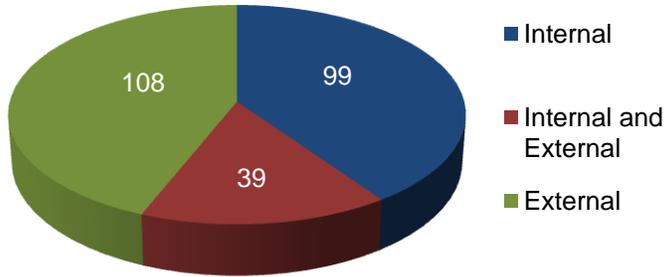
Responding agencies report that 82% of the County's operating systems or architecture types are Microsoft Windows based.

Survey responses indicate that 51 (25%) of the County's applications are over 10 years old, including the County's Financial System, portions of the Treasurer's System, and the Jail Management System.

#### Software Applications Grouped by Implementation Dates



### Development Approach



Responding agencies report that approximately 56% of County application development is performed internally or in conjunction with external vendors.

Vendor viability is the vendor's ability to stay in business. Agencies report that 65% of third-party applications are developed or supported by vendors with strong viability.

### Vendor Viability

