



A Report  
to the  
Board of  
Supervisors

*Maricopa County  
Internal Audit  
Department*

**Ross L. Tate**  
County Auditor

---

# Countywide Data Centers and Disaster Recovery

*71% of Data Center Controls Reviewed  
Were Operating as Intended*

---

March ■ 2009

Executive Summary	1
Introduction	3
Physical Security	7
Data Backup	10
Equipment Protection	14
Environmental Controls	16
Disaster Recovery Planning	19
Operations Controls	22
Appendices	25

**The mission of Maricopa County** is to provide regional leadership and fiscally responsible, necessary public services so that residents can enjoy living in a healthy and safe community.

**The mission of the Internal Audit Department** is to provide assistance to the Board of Supervisors so they can ensure Maricopa County government is accountable to its citizens.

The County Auditor reports directly to the Maricopa County Board of Supervisors, with an advisory reporting relationship to the Citizen's Audit Advisory Committee.

**Audit Team Members**

Eve Murillo, Deputy County Auditor

Toni Sage, IT Audit Supervisor

Susan Adams, Senior IT Auditor

Nic Harrison, Associate IT Auditor

Scott Jarrett, Associate Auditor

Protiviti Inc.

**Maricopa County Internal Audit**

**301 West Jefferson Suite 660**

**Phoenix, AZ 85003**

**(602) 506-1585**

[www.maricopa.gov/internal\\_audit](http://www.maricopa.gov/internal_audit)

*"Do the Right Things Right!"*



# Maricopa County

Internal Audit Department

301 West Jefferson St  
Suite 660  
Phx, AZ 85003-2143  
Phone: 602-506-1585  
Fax: 602-506-8957  
www.maricopa.gov

March 9, 2009

Max Wilson, Chairman, Board of Supervisors  
Fulton Brock, Supervisor, District I  
Don Stapley, Supervisor, District II  
Andrew Kunasek, Supervisor, District III  
Mary Rose Wilcox, Supervisor, District V

We have completed our review of information technology data centers located throughout the County. This audit was performed in accordance with the annual audit plan approved by the Board of Supervisors. To complete this work, we visited 27 data centers managed by 14 agencies, and reviewed up to 82 controls at each center for a total of approximately 2,000 controls reviewed. Control categories included: physical security, data backup, equipment protection, environmental, disaster recovery planning, and operations.

Highlights of this report include the following:

- 71% of controls reviewed were operating as intended
- 433 total improvement recommendations were issued across 14 agencies
- Several agencies reviewed are using best practices

Within this report you will find an executive summary and specific information on the areas reviewed. We appreciate the excellent cooperation provided by management and staff. If you have any questions, or wish to discuss the information presented in this report, please contact Eve Murillo, Deputy County Auditor, at 506-7245.

Sincerely,

A handwritten signature in cursive script that reads "Ross L. Tate".

Ross L. Tate  
County Auditor

# Executive Summary

## **Physical Security (Page 7)**

We tested 15 physical security controls at 27 County data center sites and found numerous weaknesses. These weaknesses increase the risk of business disruption due to unauthorized use, destruction, or theft of computer equipment or data. Using an IT Governance framework, County management should strengthen its Electronic Information Resource Security Policy with physical security guidelines for existing facilities, design standards for new construction, and requirements for new lease agreements.

## **Data Backup (Page 10)**

County data centers follow basic backup and recovery practices; however, countywide policies and procedures are lacking and key areas have weaknesses. Many IT organizations are not sending incremental data backups offsite daily or routinely testing full system restoration. Frequent data backup and routine system restoration testing prevent data loss or destruction, service interruption, and the inability to recover systems and data after a disaster. County management should establish basic policies, procedures, and standards for critical backup and restoration processes, and strengthen the control environment to match these standards.

## **Equipment Protection (Page 14)**

We tested 12 equipment protection controls at 27 sites. Although all data centers have uninterrupted power supply equipment, we found weak areas. These weaknesses increase the risk of business disruption due to loss of power, damage to equipment caused by power surges and sags, or unscheduled downtime due to inadequate system maintenance. County management should establish data center equipment protection guidelines that address protection from power loss, power fluctuations, inadequate maintenance, and power system testing.

## **Environmental Controls (Page 16)**

We found weaknesses in several key data center environmental controls, including some impacting safety. These weaknesses could increase the risk of endangering employees; damaging equipment, software, or data; impairing operational efficiency and reliability; or disrupting business operations. County management should establish policies, procedures, and standards for designing, implementing, and monitoring data center environmental controls.

## **Disaster Recovery Planning (Page 19)**

We tested 13 recovery controls at the 27 sites and found numerous weaknesses that increase the risk that critical systems would not recover following a disaster. Nine of the organizations have a disaster recovery plan in place; however, we found weaknesses in all recovery controls and no single IT organization had a complete set of strong recovery controls. The most prevalent weaknesses were related to a lack of recovery testing. During the audit, some IT organizations proactively addressed recovery testing issues. Aligning with an IT Governance framework, County management should strengthen the County Disaster Recovery Policy by aligning its requirements with current industry disaster recovery standards.

## **Operations Controls (Page 22)**

We tested 11 operations controls at the 27 data centers and found numerous weaknesses. These weaknesses increase the risk that data center operations are not effectively protecting County systems and data. The three most prevalent weaknesses involved inadequate policies and procedures for key data center operations (physical security, environmental controls, etc.), the lack of routine, formal data center access reviews, and the lack of routine data center control testing (security controls, environmental controls, etc.). We also found 102 instances of access to data centers granted to individuals who were not authorized by the IT director. County management should establish guidelines that address the policies, procedures, processes, and controls that govern data center operations.

# Introduction

## What are Data Centers and Why are They Critical?

Data centers house the computer equipment (servers) containing mission-critical information systems and data essential to County operations. Like bank vaults that protect valuable assets, data centers should be secure in order to ensure continuous, reliable operation. The County primarily employs two types of data center environments:

- County Operated
- Third-Party Operated – The following enterprise applications will run in outsourced data centers
  - ADP<sup>1</sup> – Human Resources and Payroll (PRISM)
  - CGI<sup>2</sup> – Financial Systems (Advantage)



**One of CGI's Data Centers**  
(Source: CGI public website)

## Scope of Review and Overall Findings

To obtain a complete view, we considered all County IT organizations. We employed questionnaires, site tours, interviews, and data testing. In each of the 27 data centers we visited, we reviewed up to 82 controls (for a total of 2,000 controls) in six categories:

- Physical Security
- Environmental Controls
- Backup and Restoration
- Equipment Protection
- Data Center Operations
- Disaster Recovery Planning

In general, the County data centers get a passing score. We found that 71% of the controls were operating as intended. Some controls, such as backing up critical data at least daily, were operating effectively across all of the sites we visited. Participating Information Technology (IT) organizations expressed interest in collaborating to establish County guidelines and best practices. We noted several agency “centers of excellence” within each of the six data center control categories that can serve as models for these initiatives. This is compatible with the County’s current IT Governance initiative. An IT governance framework can be a critical element in ensuring proper control and governance over information and the systems that create,

---

<sup>1</sup> Automated Data Processing. Ref: FY08 HRIS outsourcing project review.

<sup>2</sup> CGI, a public corporation headquartered in Canada, is one of the largest independent IT and business process service companies.

store, manipulate, and retrieve it.<sup>3</sup> Past County IT Governance initiatives (Policy A-1601) are now being reviewed and updated by the County Chief Information Officer (CIO) with the County's IT leadership.

Court Technology Services (CTS) had the strongest control environment of the sites we reviewed, with the Assessor's Office, Clerk of the Courts, Office of Enterprise Technology (OET), and the Public Works Infrastructure Technology Center (ITC) rounding out the top five.

## **Countywide Information Technology (IT) Organization**

Maricopa County's IT organization structure mirrors the County's federated model; IT organizations are generally aligned with an elected or appointed office and each elected office has one primary data center.<sup>4</sup> During our research, we found that 16 IT organizations support 46 County agencies with 23 primary data centers and four backup recovery sites.<sup>5</sup>

The data centers range in size from 2,000 square foot operations that support multiple agencies such as OET, CTS, ITC, and the Regional Development Services Agency's IT organization (RDSA), to approximately 100 square foot small operations supporting single agencies or departments, such as Animal Care and Control and the Office of the Legal Defender. In the following two instances, physical space and some controls are shared among multiple agencies, but operations are run independently:

- Assessor's Office, County Attorney's Office, and OET
- Court Technology Services (recovery site) and Clerk of the Superior Court

## **Financial Analysis**

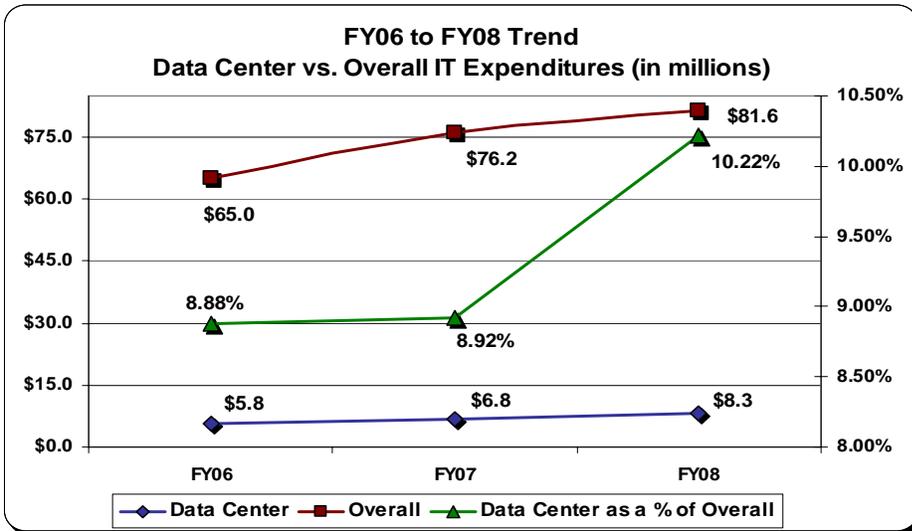
The County invests substantially in information systems; countywide FY 2008 IT expenditures totaled \$81.6 million. As the graph on the following page shows, County data center expenditures totaled \$8.3 million during FY 2008, or 10.2% of total countywide IT expenditures. This is significant increase over the prior two years. The second chart shows the increase is attributed to personnel, repair and maintenance, and general supply costs.

---

<sup>3</sup> Source: IT Governance Institute

<sup>4</sup> See Appendix A for a copy of the IT organization chart

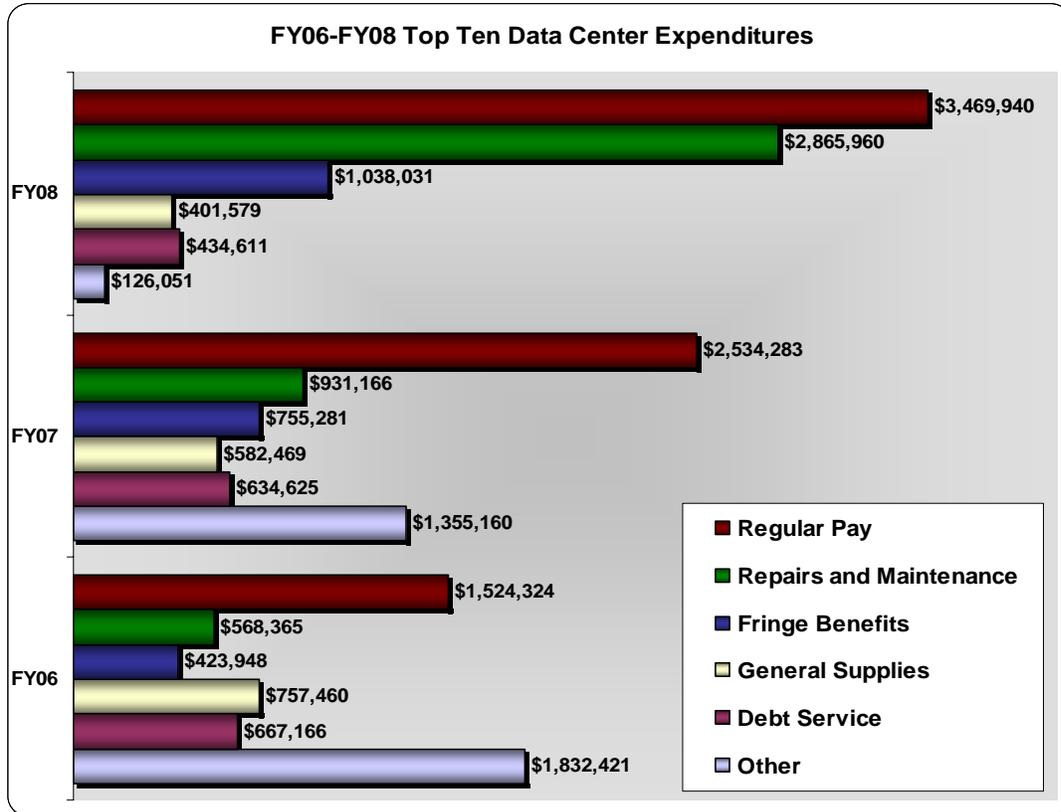
<sup>5</sup> May not include all satellite locations



SOURCE: Advantage 2.0 data, based on IA data analysis

**Above:** Data center expenditures make up an increasingly larger portion of overall IT expenditures.

**Below:** The increasing data center expenditures can be attributed to personnel (pay and benefits), repairs and maintenance, and supplies.



SOURCE: Advantage 2.0 data, based on IA data analysis

## **Scope and Methodology**

### Audit Scope

Initially, this countywide review included all agencies. However, the County Sheriff's Office and County Attorney's Office would not allow us access to their data centers. Consequently, we were unable to complete testing in these two areas.

### Audit Objectives

The objectives were to determine if County data center controls provide reasonable assurance that:

- Access to computer resources (data, equipment, and facilities) is reasonable and restricted to authorized individuals
- Sensitive information technology resources are adequately protected from environmental hazards
- System backup and recovery procedures adequately protect critical data from loss or destruction, support normal business continuity, and contribute to the disaster recovery process
- Sensitive equipment is adequately protected against loss of power, fluctuations in power, and inadequate maintenance
- Operations policies and procedures effectively support the protection and efficient operation of County systems and data
- Disaster recovery planning efforts are adequate

### Audit Timeframe

The audit included data from fiscal years 2006 through 2008.

### Auditing Standards

We conducted this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

# Issue 1 Physical Security Could Be Improved

## Summary

Adequate physical security is the first line of defense against unauthorized intrusions into the valuable data housed at County data centers. We tested 15 physical security controls at 27 County data center sites and found numerous weaknesses. These weaknesses increase the risk of business disruption due to unauthorized use, destruction, or theft of computer equipment or data. Using an IT Governance framework, County management should strengthen its Electronic Information Resource Security Policy with physical security guidelines for existing facilities, design standards for new construction, and requirements for new lease agreements.



**Camera systems monitor data center entry/exit points as part of the physical security system**

## Criteria

The County's Electronic Information Resource Security Policy (A1605) was established to ensure effective electronic information management:

“Information is a County asset and must be appropriately evaluated and protected against unauthorized use, disclosure, theft, modification, destruction, or denial of access. The protection and security of information resources is the responsibility of each elected official, appointed department director, and all employees.”

Industry has established the following widely accepted IT control framework standards:

- Control Objectives for Information Technology (COBIT), an IT best practices and general controls framework, is recognized world-wide as a useful tool for improving IT systems and processes control structure
- Federal Information System Controls Audit Manual (FISCAM), is an IT control audit methodology that aligns with generally accepted government auditing standards

See Appendix B for more detailed criteria statements.

## Condition

We tested 15 physical security controls at 27 sites and found weaknesses in these controls meant to protect County data centers. Given the criticality of data center operations, exterior physical security controls for data centers facilities often appeared lax. Some critical interior physical security controls did not provide adequate protection against plausible threats.

Condition of 15 Physical Security Controls at 27 Sites	Sites with Weaknesses	
	Number	Percentage
<b>Exterior Security</b>		
1. Weak general perimeter security	6	22%
2. Lack of exterior camera coverage	6	22%
3. Weak entry/exit point security	2	7%
4. Inadequate guard/receptionist coverage	2	7%
<b>Interior Security</b>		
5. Signage disclosed data center location	8	30%
6. Inadequate camera coverage for data center entry/exit	22	81%
7. Weak data center entry/exit point security	6	22%
8. Other sensitive IT areas not properly secured	1	4%
9. No data center-specific visitor log	22	81%
10. No restrictions for portable storage/computing devices	26	96%
11. Weak visitor escort procedures	2	7%
12. Lacking multiple layers of security	5	19%
13. Weak separation of third-party equipment	7	26%
14. Weak outside party (vendor/contractor) access restrictions	0	0%
15. Inadequate tracking of data center access keys (only applicable to 12 sites)	12 of 12	100%

## Effect

Effective physical security controls protect data centers from internal and external threats. Examples of these threats are accidental damage by inexperienced employees or careless vendors; malicious harm caused by disgruntled employees, criminals, malicious hackers; and equipment or data theft. Weak physical security leads to:

- Unauthorized use, modification, destruction, or theft of systems and data
- Unauthorized access to sensitive information
- Disruption of system and operational processing
- Threats to the safety of data center personnel

## Cause

External physical security inadequacies were primarily found at data centers located in leased facilities. As a tenant, the County has limited control over facility security measures.

Internal security weaknesses resulted from a lack of data center security standards and guidelines, and clear access authorization policies.

### **Recommendation**

Using an IT Governance framework, County management should strengthen its Electronic Information Resource Security Policy with physical security guidelines for existing facilities, design standards for new construction, and requirements for new lease agreements. Management should consider data center size and systems criticality when implementing guidelines for the following controls:

- Multiple layer exterior security—camera coverage, guards, reception area procedures
- Multiple layer interior security
  - Physical access restrictions and monitoring of employees, other County agencies, vendors, contractors, and visitors
  - Camera coverage for data center entry/exit points
  - Isolating third-party equipment in accordance with applicable agreements

Fourteen individual agency reports containing applicable findings and a total of 433 improvement recommendations were sent to IT management and their directors for response.

# Issue 2 Data Backup Could Be Improved

## Summary

County data centers follow basic backup and recovery practices, however, countywide policies and procedures are lacking and key areas have weaknesses. Many IT organizations are not sending incremental data backups offsite daily or routinely testing full system restoration. Frequent data backup and routine system restoration testing prevent data loss or destruction, service interruption, and the inability to recover systems and data after a disaster. County management should establish basic policies, procedures, and standards for critical backup and restoration processes and strengthen the control environment to match these standards.



Backup tapes in a storage rack

## Criteria

Industry has established widely accepted IT control framework standards: COBIT and FISCAM.<sup>6</sup>

## Condition

### Backup and Recovery Procedures

We tested 15 backup and recovery controls at 27 locations and found weaknesses in some critical procedures. Many IT organizations are not sending incremental data backups offsite daily or routinely testing full system restoration. Agencies are individually managing their offsite backup storage vendor relationships, leading to potential inefficiencies and higher costs for services.

Condition of 15 Tested Backup and Recovery Controls at 27 Sites	Sites with Weaknesses	
	Number	Percentage
1. Inadequate backup job scheduling	0	0%
2. Not performing daily incremental backups	0	0%
3. Not performing weekly full backups	0	0%
4. Backups are not stored offsite	3	11%
5. Offsite not secured or separated from the data center	5	19%
6. Tapes are not stored securely onsite	4	15%
7. Incremental backups not taken offsite daily	16	59%
8. Full backups not taken offsite weekly	3	11%

<sup>6</sup> See Appendix B for detailed criteria

Condition of 15 Tested Backup and Recovery Controls at 27 Sites	Sites with Weaknesses	
	Number	Percentage
9. Inadequate backup media tracking/reconciliation	5	19%
10. Tape transport to offsite storage not secure	5	19%
11. Sensitive backup data not encrypted	3	11%
12. Backup data integrity not tested prior to going offsite	8	30%
13. Single file restoration not tested regularly	2	7%
14. Full system restoration not tested regularly	16	59%
15. System state/server configuration files not backed up	1	4%

#### Backup Storage Vendor Security Controls

We tested controls at the County's two offsite backup storage vendors, Data Pros and Iron Mountain, and found both provide adequate security for backup tapes. However, while Data Pros has not commissioned an independent control assessment, Iron Mountain had an internationally known accounting firm, Ernst & Young, perform a SysTrust opinion<sup>7</sup> to provide reasonable assurance the IT infrastructure environment was protected against unauthorized physical and logical access.



**Backup tape storage boxes ready for pick up by a County vendor, Data Pros**

<sup>7</sup> SysTrust was developed jointly by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). A SysTrust engagement is performed by a licensed CPA to evaluate a system's reliability as measured against the SysTrust principles and criteria.

Report Card for Offsite Backup Procedures and Security			
	■ Good	■ Adequate	■ Could Be Improved
	Data Pros / OET	Iron Mountain / Assessor's Office	
Back Up Site Security	■	■	
Environmental Controls	■	■	
Vehicle Security	■	■	
Drop off / Pick-Up Security	■	■	
Independent Assessment of Controls	■	■	

#### Offsite Storage Costs

The County financial system shows \$63,000 in FY 2008 payments for vendor offsite tape storage. Although this is not a significant cost, agencies cited cost as the primary reason for not fully utilizing offsite storage. The vendor maintains separate agency accounts and bills separately, increasing the risk of duplicate service fees.

#### Unannounced Inspections

We performed surprise tape transfer inspections at OET and at the Assessor's Office; no exceptions were noted.

#### **Effect**

Inadequate backup and restoration procedures could result in loss or destruction of data, service interruption, and the inability to recover systems and data in the event of a disaster. Agencies individually managing their offsite backup storage vendor relationships may incur inefficiencies and higher costs for services. When agencies individually negotiate pricing for offsite backup storage services under the current "umbrella" contracts, the County cannot leverage its overall size to gain economies of scale and reduce costs or increase service levels. For example, one offsite storage vendor offers a reduced price per transaction if certain transaction volumes are processed annually.

#### **Cause**

The County lacks effective backup and restoration policies, procedures, or basic standards. County management has not identified responsibility for developing these standards. The County is not managing offsite storage as a countywide process.

## **Recommendation**

Using the IT Governance meetings as a forum, IT directors should coordinate countywide offsite storage to maximize service and minimize cost. Using an IT Governance framework, County management should establish policies, procedures, and standards for backup and restoration procedures. Backup and restoration procedures should include the following areas:

- Backup schedules
- Secure storage and transport
- Data encryption requirements
- Testing requirements
- Availability of system state/server configuration for recovery of critical systems

Fourteen individual agency reports containing applicable findings and a total of 433 improvement recommendations were sent to IT management and their directors for response.

# Issue 3 Equipment Protection Could Be Improved

IT equipment houses and processes critical data and needs protection from power loss, power fluctuations, and equipment failure. We tested 12 equipment protection controls at 27 sites. Although all data centers have uninterrupted power supply equipment, we found weak areas. These weaknesses increase the risk of business disruption due to loss of power, damage to equipment caused by power surges and sags, or unscheduled downtime due to inadequate system maintenance. The two most prevalent weaknesses involved agencies not performing routine backup power systems testing and locations lacking sufficient backup generator power. County management should establish data center equipment protection guidelines that address protection from power loss, power fluctuations, inadequate maintenance, and power system testing.



**A large, sophisticated backup power system based on chemical storage batteries**

## Criteria

Industry has established widely accepted IT control framework standards: COBIT and FISCAM.<sup>8</sup>

## Condition

We tested 12 protection controls at 27 sites and found numerous weaknesses. These weaknesses increase the risk of business disruption due to loss of power during peak business hours, damage to equipment caused by power surges and sags, or unscheduled downtime due to inadequate system maintenance. The two most prevalent weaknesses involved agencies not performing routine backup power systems testing and locations lacking sufficient backup generator power.

Condition of 12 Tested Equipment Protection Controls at 27 Sites	Sites with Weaknesses	
	Number	Percentage
1. No Uninterrupted Power Supply (UPS) system in place	0	0%
2. UPS does not support graceful systems shutdown	0	0%

<sup>8</sup> See Appendix B for detailed criteria

Condition of 12 Tested Equipment Protection Controls at 27 Sites	Sites with Weaknesses	
	Number	Percentage
3. UPS not tested on a regular basis	7	26%
4. Data center is not connected to a backup generator	10	37%
5. Generator was not proven capable of handling system load	10	37%
6. Backup generator not maintained or regularly tested	10	37%
7. No reserve generator fuel supply plan for long outage	10	37%
8. No power conditioning to protect from spikes or sags	1	4%
9. No redundant power path to the equipment	8	30%
10. Clutter near sensitive equipment that could cause damage	5	19%
11. Working equipment sitting unused and not salvaged	1	4%
12. Equipment not properly maintained (out of warranty, etc.)	1	4%

### Effect

Weaknesses in equipment protection measures increase the risk of business disruption due to loss of power during peak business hours, damage to equipment caused by power surges and sags, or unscheduled downtime due to inadequate system maintenance. Batteries in UPS systems degrade over time and without routine testing, the batteries might fail during an actual power outage.

### Cause

IT management is aware of the need for a long-term backup power solution, but either lacked the funds to connect to a generator or was limited by facility lease constraints. The County lacks policies, procedures, or standards to sufficiently guide IT management. Compounding the problem is that no party has the clearly defined responsibility to create these guidelines.

### Recommendation

County management should establish data center equipment protection guidelines that address protection from power loss, power fluctuations, and inadequate maintenance. These guidelines should include:

- Uninterrupted Power Supply testing to support graceful shutdowns and backup generator to support critical systems—testing, load capacity, preventive maintenance, refueling
- Clean power (no surges, spikes, sags, etc.) and dual-power pathways to equipment
- Keeping the area around sensitive equipment clear to avoid accidental damage
- Preventive maintenance per manufacturer guidelines and warranty coverage on sensitive equipment (if determined feasible through cost-benefit analysis)

Fourteen individual agency reports containing applicable findings and a total of 433 improvement recommendations were sent to IT management and their directors for response.

# Issue 4 Environmental Controls Need Improvement

## Summary

We found weaknesses in several key data center environmental controls, including some impacting safety. These weaknesses could increase the risk of endangering employees, damaging equipment, software, or data; impairing operational efficiency and reliability; or disrupting business operations. County management should establish policies, procedures, and standards for designing, implementing, and monitoring data center environmental controls.

## Criteria

Industry has established widely accepted IT control framework standards: COBIT and FISCAM.<sup>9</sup>

## Condition

We tested 16 environmental controls at 27 sites and found weaknesses in several key data center controls meant to protect sensitive IT equipment. Many of the inspected data centers were unnecessarily exposed to fire and flood risks, with few controls to mitigate the risks.



**Good cable management can increase installation efficiency, improve airflow, and prevent hot spots**



**New environmentally-friendly halon suppression systems can stop fires without damaging equipment.**

<sup>9</sup> See Appendix B for detailed criteria

Condition of 16 Tested Environmental Controls at 27 Sites	Sites with Weaknesses	
	Number	Percentage
<b>Air Conditioning</b>		
1. Inadequate cooling system	5	19%
2. Improper airflow/hot spots near equipment	3	11%
3. Improper relative humidity	0	0%
4. Lack of temperature monitoring with alerts	8	30%
5. Lack of humidity monitoring with alerts	15	56%
<b>Fire Protection</b>		
6. No fire suppression system in place	3	11%
7. Fire suppression system not regularly tested	2	7%
8. Flammable clutter near equipment	6	22%
9. No hand-held extinguisher present	7	26%
10. No fire protection in construction	16	59%
<b>Water Protection</b>		
11. Facing natural hazards with no mitigation	5	19%
12. Data center located in a flood plain	6	22%
13. Equipment not on raised flooring or racks	19	70%
14. Data center located on the ground floor or in basement	17	63%
15. Lack of leak sensors with alerts	23	85%
<b>Human Hazards</b>		
16. Food, drink, or smoking not prohibited in the data center	7	26%

## Effect

Environmental controls protect people and sensitive IT equipment from fire, water damage, natural and man-made disasters, air conditioning failure, food/drink/smoke damage, and harmful levels of dust and debris. Environmental controls weaknesses could:

- Endanger employees
- Damage or destroy equipment, software, and data
- Impair operational efficiency and reliability
- Disrupt or close business activity if business continuity plans are non-existent or inadequate

## **Cause**

Many of the inspected data centers were established years ago under an old paradigm of data center design. Often, the IT directors did not oversee the design of key environmental controls, such as data center location or construction methods/materials.

The County lacks policies, procedures, or basic standards on protecting the data center from environmental hazards. County management has not identified responsibility for developing these standards.

## **Recommendation**

County management should establish policies, procedures, and standards for designing, implementing, and monitoring data center environmental controls that include:

- Air conditioning
  - Ensuring adequate cooling and humidity control systems with alerts
  - Maintaining proper airflow with no obstructions/hot spots near equipment
- Fire protection
  - Providing adequate fire suppression system and accessible hand-held extinguisher
  - Ensuring areas near equipment are kept free of flammable clutter
  - Designing fire protection measures in construction
- Water protection
  - Locating data centers outside of flood plains
  - Keeping sensitive equipment in locations above the ground floor and equipment on raised flooring or racks
  - Installing leak sensors on the data center floor with alerts
- Human hazards
  - Prohibiting eating, drinking, or smoking in the data center

Fourteen individual agency reports containing applicable findings and a total of 433 improvement recommendations were sent to IT management and their directors for response.

# Issue 5 Disaster Recovery Plans Should Be Reviewed and Tested

## Summary

Effective disaster recovery planning helps ensure that critical information systems can be restored following a disaster. We tested 13 recovery controls at the 27 sites and found numerous weaknesses that increase the risk that critical systems would not recover following a disaster. Nine of the organizations have a disaster recovery plan in place, however we found weaknesses in all recovery controls and no single IT organization had a complete set of strong recovery controls. The most prevalent weaknesses were related to a lack of recovery testing. During the audit, some IT organizations proactively addressed recovery testing issues. Aligning with an IT Governance framework, County management should strengthen the County Disaster Recovery Policy by aligning its requirements with current disaster recovery standards.

## Criteria

The County’s Disaster Recovery Plan Policy (A1602) was established to protect critical data:

“Each elected official and appointed department director shall establish their Disaster Recovery Plan(s) and practices sufficient to ensure that: 1) their information resources are protected, backed-up, and recoverable; and 2) that the integrity, availability, and reliability of all electronic assets are not compromised or affected.”

Industry has established widely accepted IT control framework standards: COBIT and FISCAM.<sup>10</sup>

## Condition

We tested 13 recovery controls at the 27 sites and found numerous weaknesses. These weaknesses increase the risk that critical County systems would not be able to recover following a disaster. Nine of the 14 County IT organizations managing the 27 sites have a disaster recovery plan in place, however we found weaknesses in all disaster recovery controls, and none of the IT organizations had a complete set of strong recovery controls. The most prevalent control weakness was a lack of disaster recovery testing. During the course of our audit, some IT organizations proactively addressed disaster recovery testing issues.

Condition of 13 Tested Controls at 14 Agencies	Sites with Weaknesses	
	Number	Percentage
1. No disaster recovery plan (DRP) in place	3	21%
2. DRP is not updated on a regular basis	11	79%

<sup>10</sup> See Appendix B for detailed criteria

Condition of 13 Tested Controls at 14 Agencies	Sites with Weaknesses	
	Number	Percentage
3. DRP is not approved by both business and IT management	7	50%
4. DRP does not include disaster definition or assign responsibility for declaring a disaster	6	43%
5. DRP does not identify the critical processes, people, and IT infrastructure required to recover from a disaster	5	36%
6. DRP is not formally communicated to affected parties	10	71%
7. DRP has not been tested	11	79%
8. DRP not tested after system changes	12	86%
9. DRP not updated as needed after testing	12	86%
10. Disaster recovery site not established	7	50%
11. Disaster recovery site is exposed to same risks as the primary site	9	64%
12. Disaster recovery site is not prepared for recovery in accordance with the DRP	9	64%
13. DRP activities are not documented	8	57%

### Effect

Weak disaster recovery planning efforts increase the risk that the County will not be able to recover critical data and IT processing following a disaster. Inadequate or non-existent disaster recovery plans increase the risk that County business operations will not be able to function because systems will not be recoverable in the event of a disaster.

### Cause

IT management is aware that detailed, formal disaster recovery processes are needed and is seeking countywide guidance for help in establishing disaster recovery plans. Currently, the County has a high-level policy and disaster recovery plan template that could help guide individual IT organizations in aligning their own disaster recovery planning efforts with best practices and County standards. However, both the policy and template are out-of-date and may not be useful to County IT management.

### Recommendation

County management should strengthen the County disaster recovery policy by adding guidelines that align County disaster recovery planning requirements with current industry standards. These guidelines should include:

- Regularly reviewing, updating, and communicating the disaster recovery plan
- Ensuring business leaders and IT management involvement and approval
- Defining “disaster” and assigning responsibility for declaration

- Identifying processes, people, and IT infrastructure required to recover critical systems
- Establishing a plan testing methodology to follow after major infrastructure changes
- Establishing a recovery site (hot/warm/cold site, reciprocal processing agreement, third-party recovery services, etc.) that is not exposed to the same risks as the primary data center and is adequately prepared for recovery
- Tracking and reporting unplanned incidents

Fourteen individual agency reports containing applicable findings and a total of 433 improvement recommendations were sent to IT management and their directors for response.

# Issue 6 Data Center Operations Could Be Improved

## Summary

Strong controls over data center operations safeguard valuable County data and keep the data center running efficiently and effectively. We tested 11 operation controls at the 27 data centers and found numerous weaknesses. These weaknesses increase the risk that data center operations are not effectively protecting County systems and data. The three most prevalent weaknesses involved inadequate policies and procedures for key data center operations (physical security, environmental controls, etc.), the lack of routine, formal data center access reviews, and the lack of routine data center control testing (security controls, environmental controls, etc.). We also found 102 instances of access to data centers granted to individuals who were not authorized by the IT director. County management should establish guidelines that address the policies, procedures, processes, and controls that should govern data center operations.

## Criteria

Industry has established widely accepted IT control framework standards: COBIT and FISCAM.<sup>11</sup>

## Condition

### Data center operations

We tested 11 operation controls at the 27 sites and found numerous weaknesses. The three most prevalent weaknesses were inadequate policies and procedures for key data center operations (physical security, environmental controls, etc.), the lack of routine data center control testing (security controls, environmental controls, etc.), and the lack of routine, formal data center access reviews.

Condition of 11 Tested Data Operations Controls at 27 Sites	Sites with Weaknesses	
	Number	Percentage
1. Inadequate equipment/service hosting controls	1	4%
2. Lack of or inadequate data center policies and procedures	15	56%
3. Data center physical access not formally reviewed	16	59%
4. Data center physical access not properly restricted (only applicable to 7 sites)	7 of 7	100%
5. Lack of or inadequate after hours support system	0	0%
6. Lack of uptime monitoring/excessive downtime	1	4%
7. Data center controls not tested	21	78%

<sup>11</sup> See Appendix B for detailed criteria

Condition of 11 Tested Data Operations Controls at 27 Sites	Sites with Weaknesses	
	Number	Percentage
8. Lack of or inadequate policy and procedure communication	12	44%
9. Inappropriate data center access control for third-parties	2	7%
10. System state/server configuration not recorded	0	0%
11. Inadequate segregation of duties over data center security	2	7%

### Badge access controls

We reviewed a sample size of four agencies' physical access logs and found several instances of unauthorized access. We also tested a judgmental sample of badge access authorizations within the four agencies. We found 102 instances where individuals with access to data centers did not have IT managers' written authorization. Although IT managers may have internal processes in place to review and approve data center access for their agencies, Protective Services controls the badge access system and can modify data center access without the agencies' knowledge.

Sample Test -- Protective Services Reported Data Center (DC) Badge Access Compared to IT Director Authorization				
Agencies*	IT Staff	Individuals with IT Director Approved Access	# of Individuals with Badge Access Capability, but Not Approved by IT Director	
			Individuals with Access Capability who did Not Attempt Access	Individual Gained Access
Recorder's Office	27	56	0	0
Court Technology Services	100	26	25	1
Clerk of the Courts	34	66	0	0
Public Defender's Office	8	8	76	0
*Note: Office of Enterprise Technology (OET) was selected for sample testing but, at the time of the audit, OET shared a data center room with Maricopa County Attorney's Office (MCAO) and we were denied access to MCAO controlled records and reports.				

### **Effect**

Inadequate or non-existent policies and procedures for key data center operations (physical security, environmental controls, etc.) increase the risk that data center operations may not be effectively protecting County systems and data.

### **Cause**

IT managers are aware of the need for policies, procedures, and controls to govern data center operations and are seeking countywide-level guidance for help in establishing these frameworks.

Currently, the County does not have any high-level policies, procedures, or standards to guide individual IT organizations in aligning their data center operations with best practices and County standards.

Facilities Management and Protective Services personnel data center access may be excessive because the County lacks formal assignment of responsibility for who can grant data center access.

### **Recommendation**

Using the IT Governance meetings as a forum, IT management should work with Protective Services to establish a County policy and associated procedures for authorizing, granting, and monitoring access to County data centers. Using an IT Governance framework, IT management should establish process and control guidelines for governing data center operations. These guidelines should include:

- Segregating duties in relation to physical security (no one individual with the authority to grant, revoke, and modify access rights)
- Restricting third-parties from accessing the data center (escort at all times)
- Establishing an emergency response system and communicating it to users
- Establishing goals for critical system uptime, formally monitoring uptime, and developing techniques to reduce downtime
- Establishing adequate data center controls (security, environmental, etc.), testing these controls and documenting the results
- Recording and updating critical system configuration files

Fourteen individual agency reports containing applicable findings and a total of 433 improvement recommendations were sent to IT management and their directors for response.

# Appendix A

## County IT Organizations and Supported Agencies



### Chart Key

**IT Organization Name  
(or agency if no consolidated IT)**

*Supported department 1  
Supported department 2  
Supported department 3  
Etc.*

# Appendix B

## Criteria

We developed audit criteria by applying detailed security, control, and audit frameworks to the general guidance of County policies regarding information security and disaster recovery planning. County policies A1605 – Electronic Information Resource Security, and A1602 – Disaster Recovery, outline the management-level responsibilities and general requirements of County information security and disaster recovery planning efforts. We used industry standard IT control frameworks, Control Objectives for Information and Related Technology (COBIT) and Federal Information System Controls and Audit Manual (FISCAM), as guidance to develop detailed audit procedures that ensure adequate compliance with County policy. See the following websites for more information:

[www.isaca.org/cobit](http://www.isaca.org/cobit)

<http://www.gao.gov/special.pubs/fiscam.html>

## County Policies

County policy **A1605 - Electronic Information Resource Security** states:

*Information is a county asset and must be appropriately evaluated and protected against unauthorized use, disclosure, theft, modification, destruction, or denial of access. The protection and security of information resources is the responsibility of each elected official, appointed department director, and all employees.*

*Each elected official and appointed department director shall establish security controls and practices sufficient to ensure that confidentiality (to the extent required by law), integrity, availability, and appropriate use of all electronic data and information assets will be maintained for information systems...*

*Elected officials and appointed department directors shall:*

- *Adopt a department specific security policy and submit to the Electronic Information Resource committee*
- *Establish security controls sufficient to ensure the confidentiality, integrity, availability, and use of electronic information resources for which they have responsibility. Departmental standards, procedures and practices developed for the protection of County electronic information resources must be consistent with the Maricopa County Security Standards Manual*
- *Establish a security officer function within their department. The protection of electronic information resources and information systems are part of that individual's responsibilities.*
- *Conduct security awareness programs for all their employees*
- *Perform periodic assessments of the vulnerability of their electronic information resources and information systems to internal and external threats that may cause destruction, modification, denial of access, and/or unwarranted disclosure...*

County policy **A1602 – Disaster Recovery** states:

*Each elected official and appointed department director shall establish their Disaster Recovery Plan(s) and practices sufficient to ensure that: 1) their information resources are protected, backed-up, and recoverable; and 2) that the integrity, availability, and reliability of all electronic assets are not compromised or affected. Each department shall:*

- *Identify business operations or information technology resources that are at risk*
- *Develop and maintain plans that enable short and long term recovery of IT systems*
- *Include sufficient detail to enable full resumption of normal operations*
- *File plans with Emergency Management and the Office of the Chief Information Officer (OCIO)*
- *Comply with reviews of Internal Audit*
- *Train staff to efficiently and effectively execute Disaster Recovery Plans*
- *Test Disaster Recovery Plans and emergency procedures*
- *Track, record, and report all disaster recovery activities*
- *Respond to all public inquiries about such incidents...*

### **IT Frameworks**

Control Objectives for Information and Related Technology (COBIT) is a framework of IT best practices and general controls that is recognized world-wide as a useful tool for improving the control structure of IT systems and processes. Organizations that have realized success through using COBIT include:

- U.S. House of Representatives
- Sun Microsystems
- Allstate
- Charles Schwab
- Maricopa County Court Technology Services (CTS)

Federal Information System Controls Audit Manual (FISCAM) provides a methodology for performing IT control audits in accordance with “generally accepted government auditing standards” (GAGAS), as presented in *Government Auditing Standards* (also known as the “Yellow Book”).

Both COBIT and FISCAM recommend establishing policies, procedures, and controls to:

- Ensure physical security
- Provide protection against environmental hazards
- Ensure that critical data and systems are backed up and can be restored
- Protect sensitive equipment from power anomalies and inadequate maintenance
- Ensure the efficiency and effectiveness of data center operations
- Provide assurance that critical systems can be recovered in a disaster