MARICOPA COUNTY INTERNAL AUDIT

General Controls Questionnaire

	Control Consideration	Yes	No	N/A	Remarks
	MANAGEMENT CONTROLS				
1.	Is top level management or appropriate County leadership involved in monitoring information systems projects and resource priorities?				
2.	Describe your 3-5 year plan for IT.				
3.	What is your annual budget for IT?				
4.	Has the IT area been audited before?				
a.	Is there evidence of effective actions to follow-up on past audit recommendations?				
5.	Obtain an organization chart. Is there adequate separation of duties within the IT operation? The following functions are usually performed by a different individual or group:				
a.	System analysis				
b.	Application programming				
c.	Acceptance testing				
d.	Program change control				
e.	Data control				
f.	Source transaction origination				
g.	System software maintenance				
h.	Computer files maintenance				
I.	Computer equipment operations				
8	Is the IT manager aware of problems and weaknesses in controls?				
9	Are there areas that the IT manager would like to see addressed in the IT audit?				

	Control Consideration	Yes	No	N/A	Remarks
	ACCESS CONTROLS				
	PHYSICAL SECURITY				
1.	Are physical access devices (i.e., card-key or combination lock) used to restrict entrance to the computer room?				
2.	Is the physical location of the computer room appropriate to ensure security?				
3.	Ensure that proper temperature controls and an uninterrupted power supply (UPS) are functioning effectively.				
4.	Review adequacy of fire detection and fire extinguishing system.				
5.	For any other sensitive areas, are access controls to these areas adequate? Examples of other sensitive areas include communications closets, any UPS equipment, and tape libraries.				
6.	Is capacity planning and performance monitoring performed to ensure adequate system service levels?				
7.	Is problem tracking adequate to ensure that all problems get reported and resolved in a timely manner? How is this monitored?				
	LOGICAL ACCESS				
8.	Is there a security policy users must sign to get computer access?				
9.	Is there a security officer appointed?				
a.	Does the security officer ensure that available features have been implemented? (e.g., application security, and database security)?				
10.	Are passwords changed periodically?				
11.	Is there a minimum password length?				

	Control Consideration	Yes	No	N/A	Remarks
12.	Is user access based on written authorization and given on a need-to-know basis?				
13.	Is file maintenance a separate access privilege?				
a.	Is maintenance restricted to a minimum number of persons and is it properly approved and reviewed?				
14.	How is access to programs and data by IT staff controlled?				
15.	Are methods in place to detect security violations?				
a.	Can security restrictions be overridden?				
16.	Are user IDs suspended after a specific number of unsuccessful attempts to gain access?				
17.	Can programmers access live files to test new programs?				
18.	Is modem access protected by a secure system, such as call-back?				
19.	Are modem numbers changed periodically?				

	Control Consideration	Yes	No	N/A	Remarks
	PROGRAM CHANGE CONTROLS				
1.	Do documented program change control procedures exist?				
2.	Are program change authorization forms used and authorized by user management before proposed program changes are made?				
3.	Are users involved in testing and sign-off of program changes?				
4.	Are changes moved to production by someone other than application programmers?				
5.	Is adequate documentation maintained to support all program changes?				
6.	Does the auditee use library control software to manage source programs and object programs?				
7.	Is program documentation updated as changes are made?				
8.	Does the auditee have procedures for emergency program changes?				

	Control Consideration	Yes	No	N/A	Remarks
	BACKUP AND RECOVERY CONTROLS				
1.	Are critical files and programs regularly copied to tapes or cartridges to establish a generation of files for audit trail purposes and removed to off-site storage to ensure availability in the event of a disaster?				
2.	Are tape inventory logs used and compared to the contents of the off-site facility to verify that the appropriate backup files are being maintained?				
3.	Are controls in place at the off-site storage location to ensure that it is fireproof and secure?				
	DISASTER RECOVERY PLAN				
4.	Does the auditee have a documented disaster recovery plan for processing critical jobs in the event of a major hardware or software failure?				
a.	Has the disaster recovery plan been updated on a regular basis?				
b.	Has the recovery plan been tested?				
5.	Is the disaster recovery plan maintained off-site and updated when changes occur?				
6.	Does the backup and recovery plan include:				
a.	Personnel assigned to disaster teams with operating procedures and emergency phone numbers to reach them?				
b.	Arrangements for a designated physical facility?				
c.	A risk analysis identifying the critical applications, their exposures, and an assessment of the impact on the entity?				
d.	Arrangements with vendors to support the needed hardware and software requirements?				
e.	Forms to use in case of a disaster?				

	Control Consideration	Yes	No	N/A	Remarks
	SYSTEM DEVELOPMENT AND ACQUISITION CONTROLS				
1.	Interview IS management to determine whether: 1) any new computer applications were either developed in-house or acquired from a vendor, or 2) are being planned or investigated during the current audit period.				
2.	Did the auditee's procedures for developing new applications include:				
a.	System requirements analysis?				
b.	System specifications?				
c.	Technical design?				
d.	Technical procedure development?				
e.	User procedure development?				
f.	System and acceptance testing?				
g.	Transition?				
3.	Were user personnel involved in new systems development, particularly during design, development, testing, and conversion?				
4.	Were audit and security concerns considered during the initial analysis phase? (If auditee has an internal audit staff, were internal auditors involved in new system development?)				
5.	Did IT management adequately document:				
a.	Systems documentation?				
b.	Program documentation?				
c.	Operations documentation?				
d.	User documentation?				
6.	Was a post-implementation review performed to assess the success of the project?				

	Control Consideration	Yes	No	N/A	Remarks
	DATABASE CONTROLS				
1.	If the auditee has a Database Administrator (DBA), is there an adequate segregation of duties maintained among the following groups:				
a.	DBA and Application programmers?				
b.	DBA and Security administrator?				
c.	DBA and Systems programmers?				
2.	Are DBMS security features used to protect data against unauthorized access?				
3.	Are DBMS utilities and commands restricted to those responsible for the maintenance of the DBMS (usually a designated DBA)?				
4.	For change control procedures for the Data Dictionary and DBMS:				
a.	Is proper authorization obtained prior to modifications?				
b.	Are modifications tested?				
c.	Are modifications reviewed and approved?				
d.	Are changes documented?				
5.	Is the database and its data backed-up on a regular basis, and are backups secured off-site?				