Process	Sub-Process	What (Objective)	Why (Risk or Exposure)	RETURN TO MENU How (Applicable Controls)	Control Number
K Information Technology	K7 Program and System Operations	Backup and recovery procedures exist to ensure timely recovery of application data and information systems.	Without an effective and tested backup and recovery plan, it may not be possible to properly restore systems and data in the event of a disruption.	A backup and recovery plan (addressing activities such as backup frequency, job monitoring, restores, and off-site storage) is documented and reviewed periodically.	K7-1.1.1
				The backup / storage frequency is based upon system and data criticality. System owners monitor and verify the backup strategy is appropriate and executed as intended.	K7-1.1.2
				The backup and recovery plan is tested and any deficiencies are documented and addressed in a timely manner.	K7-1.1.3
				Testing of the backup media is appropriate to the system and data criticality.	K7-1.1.4
				Portable storage media should be labeled. Backups should be stored separately from originals off-site.	K7-1.1.5
				Removable storage media is protected from unauthorized access, critical data encrypted, and disposed of properly.	K7-1.1.6
		Equipment is protected by environmental controls.	Without the proper environmental controls, damage to equipment may occur and result in system downtime.	Depending on system criticality, physical facilities are equipped with adequate environmental controls to maintain systems and data, and are monitored to ensure the environmental controls function properly. (Examples are ensuring the fire suppression system is inspected, the uninterrupted power service (UPS) power backup functions normally, the temperature and humidity is within defined system specifications.)	K7-2.1.1
		Controls are in place to provide reasonable assurance that batch jobs and scheduled processes execute in a timely and appropriate manner and that variances are investigated and resolved.	Data may not be updated or calculated timely and produce unreliable results.	IT Operations ensure batch jobs, interfaces and programs execute successfully and that errors or failures are investigated, resolved and communicated timely to the department (business) / function.	K7-3.1.1
				Modifications to batch job schedules are approved and follow established change management procedures.	K7-3.1.2
		A process is in place to identify incidents and to determine if the incident potentially impacts the control environment.	Without an effective Incident Response process, there is exposure to damage, loss, modification, and unauthorized use of data.	Procedures are established and documented for Log Monitoring and Incident Response (i.e., thresholds of what constitutes an incident, a time for response, people responsible and an escalation plan) and are reviewed periodically.	K7-4.1.1
				Incidents are identified and communicated timely to the department (business) / function for appropriate action.	K7-4.1.2
				Logs that support the integrity of the system maintenance / availability logs (ex. - table size, CPU utilization, down-time alarms) and the security of the System / Subsystem / Device (ex. - event, security, operating system, substitute user (SU) logs, etc.) are monitored and reviewed, so that exceptions are investigated and resolved.	K7-4.1.3
				A County approved anti-virus software program is installed and enabled on all applicable servers which connect to a County LAN. All servers have current versions of anti-virus software and definition files installed and are updated at a frequency consistent with published County IS standards. Identification of a virus or suspected virus must be reported to, and recorded and analyzed by IT management.	K7-4.1.4
		Changes are authorized and operate as designed and continue to meet internal control requirements prior to being introduced into the production environment.	Unauthorized changes could result in reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both and may result in damage, loss, or erroneous modification of data.	Change control procedures (addressing activities such as a back out plan, test plan, testing of changes in a development environment, emergency procedures and appropriate sign-off by the owners of the devices or management) are established, documented, and reviewed periodically.	K7-5.1.1
				Changes to the production environment of critical systems (such as data, new functionality, new systems, and emergency changes) are authorized by the business or function, in accordance with documented change control procedures.	K7-5.1.2
				All changes are made to a copy of the program, tested in a segregated environment, and approved by management before moving into production.	K7-5.1.3
				System generated or manual change control logs are maintained, monitored, and suspicious activity is investigated and resolved.	K7-5.1.4
				User and application documentation is updated to reflect all program changes.	K7-5.1.5
		Data transferred between systems is accurate and complete.	Data may not be transmitted between systems completely or accurately.	Documented procedures are in place to identify and notify of missing, duplicate, redundant, or invalid data.	K7-6.1.1
				Data transmission errors are logged, impact assessed, and notification is performed timely based on the critically of the system and application.	K7-6.1.2
				Encryption is used to store and transmit data based upon the County IS policy (this includes non-County employees).	K7-6.1.3

K Information Technology	K7 Program and System Operations	System and Application software is appropriate, updated and integrated within the production environment.	Obsolete software may be easily exploited, contain processing errors, lack functionality, compatibility and stability.	New versions of existing software or additional software is tested prior to implementation on servers to ensure the software is legitimate, County approved and performs without causing unexpected negative impact over computer / network performance.	K7-7.1.1
				For new software and software updates identified to be installed on critical IT infrastructure, integrity testing is performed prior to implementation (especially on critical systems). Testing will include load tests as appropriate to the systems function and criticality. The testing is performed in isolation and checked for viruses.	K7-7.1.2
				There is a documented and established process in place that, before a system / application is added into the IT environment, it is configured according to County IS / technical standards.	K7-7.1.3
				Management periodically reviews system/device compliance with County IS standards.	K7-7.1.4
				IT infrastructure is monitored on a periodic basis to ensure the latest software / operating system updates have been applied.	K7-7.1.5
				Only software or services appropriate to the servers' function are active.	K7-7.1.6
				IT infrastructure without the latest security software updates are updated at the next available change window, or are configured to appropriately mitigate the threat of vulnerability exploitation.	K7-7.1.7