Process	Sub-Process	What (Objective)	Why (Risk or Exposure)	RETURN TO MENU How (Applicable Controls)	Control Number
K Information Technology	K6 System Access	Access to the Data Center and/or other computer facility rooms is authorized and controlled.	Without effective security access to the Data Center and/or other computer facility rooms, damage, loss, modification, and unauthorized use of the IT assets may occur.	Physical access to the Data Center and/or other computer facility rooms is properly controlled, restricted and monitored in accordance with documented site access control procedures. Examples include periodic monitoring of access devices logs or manual logs to ensure only approved access occurred, following local site procedures for periodic review of personnel, employee escort for all visitors, etc.	K6-1.1.1
				Users are granted access to secure areas based on an approved user access request process, which is based on job responsibility.	K6-1.1.2
		System access is limited to authorized department (business) / function users in accordance with job requirements.	Unauthorized and/or inappropriate access to critical systems may result in data being inappropriately altered, destroyed or released.	Security / Access administration creates accounts and profiles and grants access in accordance with applicable standards (including unique user IDs and password change frequency).	K6-2.1.1
				Security / Access administration creates accounts, grants, modifies and removes access based on approval from the department (business) or function.	K6-2.1.2
				Privileged access to the infrastructure environment is periodically reviewed by line management to ensure account privileges are consistent with their role and business risks. Frequency of these reviews is based upon the sensitivity of the granted access.	K6-2.1.3
				Application owner and department supervisors periodically review individual roles (department (business) / functional users) versus access.	K6-2.1.4
		Access to critical applications and infrastructure is authorized and controlled.	Without effective security administration for the application and its data, there is exposure to damage, loss, modification, and unauthorized use of that data.	Security administration procedures (such as adding / removing / modifying user accounts & IT privileged access review) are established, documented, and reviewed periodically.	K6-3.1.1
				User IDs and passwords are removed or locked in a timely manner when individuals leave the County or change job responsibilities.	K6-3.1.2
				Security Administrator monitors and logs security activity, and identifies security violations, which are subsequently reported to management.	K6-3.1.3
		IT Personnel (programmers, operation, system management and database management) do not perform incompatible transactions.	Without effective segregation of duties (application privileges), there is exposure to recording of invalid transactions, which could lead to inaccurate data or personal gain.	IT personnel access to production data, programs and transactions is authorized, reviewed and monitored (including emergency production access). Critical transactions are monitored (such as SAP critical transactions).	K6-4.1.1
				Emergency production access and change procedures are documented and periodically reviewed by management.	K6-4.1.2
		The use of automated security tools and system security modules should be used and properly configured to enhance information asset security.	Without leveraging all available tools, security may be susceptible to human error and abuse.	Systems / Applications are configured to deactivate a session after a specific period of inactivity.	K6-5.1.1
				The number of failed login attempts adheres to the County IS policy.	K6-5.1.2
				A log on banner advising against unauthorized access and misuse is employed on all systems whenever possible.	K6-5.1.3