Process	Sub-Process	What (Objective)	Why (Risk or Exposure)	How (Applicable Controls)	Control Number
K Information Technology	K4 Policy and Asset Management	IT resources have the proper training and redundancy to ensure the IT environment remains controlled and resources are used effectively.	A lack of training may result in inefficiencies, data loss, and the inability to access information assets.	A process is in place to properly train personnel who are responsible for critical functions.	K4-1.1.1
				A backup has been designated for critical functions that depend on an individual's KSA (knowledge, skills, abilities).	K4-1.1.2
				Job critical functions are documented including effective instructions on how to perform critical tasks. This documentation is reviewed at least annually and updated when the functions or methods change.	K4-1.1.3
				Training and operating manuals are available for critical systems appropriate to the version and function of the system or software.	K4-1.1.4
				Training plans / actual training is documented for critical IT personnel.	K4-1.1.5
		Procedures and policies are in place, communicated and consistently followed.	IT resources may be misused, under utilized, unavailable or compromised.	Exceptions to County policies / standards are submitted by management through the exception reporting process and include reasonable justification as to why the standards do not apply. This includes any variance to an information security policy which results in a reduced level of protection.	K4-2.1.1
				Compliance monitoring practices are established by management to ensure compliance to County policies is consistent.	K4-2.1.2
		Processes are in place to procure, implement, use, inventory, support, redeploy, and dispose of IT components.	IT components may not be properly obtained, accounted for, supported or maintained.	IT Inventory is complete and descriptive. Redeployment includes data and software re-initialization. Disposition includes erasing or Degaussing magnetic storage media.	K4-3.1.1
				Before an IT component acquisition, the current inventory is checked to ensure existing resources cannot be leveraged.	K4-3.1.2
				Hardware and software acquisitions and implementations are guidelined, documented and approved by management to ensure effectiveness within the County's technical architecture / environment.	K4-3.1.3
				Non-County use of IT assets is approved by the requester's Director and the IT Director on a case by case basis and does not involve critical systems.	K4-3.1.4
		Only licensed software is used. The software licenses are followed, inventoried and maintained.	Unlicensed and unapproved software may expose the County to financial loss and data destruction.	Only licensed or otherwise authorized software is used on County owned or leased hardware. Software license agreements provided by vendors clearly define the limits of use. Violation of the license agreement is prohibited.	K4-4.1.1
				Compliance with license agreements is maintained and techniques are used, whenever possible, to ensure maintenance of compliance (such as PC redeployment procedures and software metering on servers / hosts and ongoing inventory processes).	K4-4.1.2
				In addition to personal and machine license restrictions, the County negotiates for corporate or site wide licenses with the vendor when cost effective.	K4-4.1.3