DRAFT ITAC RELIABILITY CRITICAL ISSUES

	CRITICAL ISSUE	DESCRIPTION	EXAMPLES OF THIS ISSUE	GOALS FOR THIS ISSUE	CURRENT ACTIONS TAKING PLACE TO MEET GOALS	FUTURE ACTIONS NEEDED TO MEET GOALS
1	Reliable, Centralized Backup Service	Not all critical or sensitive campus data is backed up on a regular basis by a reliable backup service. This puts university operations at risk, as well as the core mission of teaching and research.	1) There is no requirement that critical data be backed up, nor is a reliable, centralized low/no cost backup service available. 2) The current central backup system is underutilized and expensive, The cost is out of reach of most departments. 3) Many on campus do not consider backups important until they have personally lost data. (Example needed: actual data loss in a department.)	1) Require that all campus data (as defined by DMUP) be regularly and professionally backed up. 2) By December 31, 2004, develop the ability to recover and restore any campus data within 24 hours. 3) Offer fast, free, secure storage (that includes professionally managed backups) to all interested students by December 31, 2005. 4) Insure that 80% of faculty and staff have affordable, regularly scheduled backups in place by June 30, 2006.	1) A new tape backup architecture has been installed in the campus computing center. 2) A provisional Data Management Use and Protection (DMUP) policy has been adopted. 3) Current % of systems backed up = (IST-CNS central campus backup + department backup) / (total number of faculty + staff)	1) Develop a reliable storage architecture for student use that seamlessly integrates into standard desktops. 2) Acquire funding to reduce or eliminate costs to faculty and staff for a centralized backup service. 3) Ask the Data Stewardship Council to take responsibility for the data backup and retention policy. 4) Work with Cal Pact to develop a training program for all faculty, staff and students on policy and options for data backup. 5) Develop heuristics for measuring success criteria for backup, retention and restoral needs.
2	Reliable Funding	Core infrastructure and services are currently unreliably and inconsistently funded. IT funding inappropriately competes directly with academic priorities.	1) Many departments don't have an annual IT budget. 2) Many faculty machines have not been replaced in five years or more because deans and departments have cut or redeployed Commission on Computing (COC) funds. 3) Central services like Cal Agenda, are often funded for capital purchases but not operational expenses, thereby preventing software licenses from being realized and used by students.	1) Publish a definition of what "core infrastructure and services" means by February 28, 2005. 2) Publish a model identifying the minimum levels of protected funding required to support core services including remediation, daily operational and lifecycle costs by February 28, 2006.	1) IST-CNS has published a "lines of business" model that shows costs associated with network services.	1) ITAC to publish a definition of core infrastructure services. 2) Require deans and directors to include clearly delineated IT expenditures in departmental budgets. 3) Analyze funding models at peer institutions and provide concrete recommendations to the Budget office on changes to the existing funding approach.

DRAFT ITAC RELIABILITY CRITICAL ISSUES

	CRITICAL ISSUE	DESCRIPTION	EXAMPLES OF THIS ISSUE	GOALS FOR THIS ISSUE	CURRENT ACTIONS TAKING PLACE TO MEET GOALS	FUTURE ACTIONS NEEDED TO MEET GOALS
			4) When funding models do exist, like the campus network funding model, they are often under-funded or out of compliance. 5) Network funding includes a subsidized recharge rate for network operation and technology refresh but the subsidized portion has frequently been under-provided.			
3	Reliable, Physical Network Infrastructure	Network services cannot be provided over a sub-standard, unreliable physical network infrastructure composed of a variety of aging and inconsistent technologies.	1) The reliability and performance of the physical network varies greatly, with inadequate funding designated to support lifecycle equipment replacement or to enforce standards in old locations. A good example of this is Tolman Hall, where uneven funding has manifested itself in a very high-performing network in the eastern tower and a very poor network in the western tower. Server-based file storage cannot be implemented due to the inconsistent quality of our networks.	1) Publish minimum infrastructure standards for all wired and wireless networks by December 31, 2004. 2) Beginning January 1, 2005, annually publish a lifecycle plan of changes needed to keep all networks up to current standards. 3) Replace the portion of the campus network (currently 30%) that doesn't meet current minimum standards by June 30, 2007. 4) Provide network connectivity at 99.9% availability by June 30, 2007.	1) IST-CNS has published wired network standards. Unpublished wireless standards exist. 3) Riser projects are renovating the physical network infrastructure on a building-by-building basis as equipment replacement funds from the network funding model are being used to replace network electronics. However, demand perpetually exceeds available funding. 4a) Some departments are providing funding for local network upgrades. 4b) A replacement for the seismically poor and infrastructurally inadequate Evans Hall core networking facility is currently being designed. Hearst Data Center Bechtel project. 4c) The new campus computing center was designed to provide redundant network services. 4d) The campus network core,	1) IST-CNS to publish a lifecycle plan for networking equipment. 2) IS&T-CNS to publish campus wireless standards. 3) Require technical signoffs at each stage of campus capital projects. 4) Complete hub relocation project out of Evans Hall. 5) Secure departmental funds to upgrade departmental networks that are below standard.

DRAFT ITAC RELIABILITY CRITICAL ISSUES

	CRITICAL ISSUE	DESCRIPTION	EXAMPLES OF THIS ISSUE	GOALS FOR THIS ISSUE	CURRENT ACTIONS TAKING PLACE TO MEET GOALS	FUTURE ACTIONS NEEDED TO MEET GOALS
					including external connectivity, DNS, and other services is currently fully redundant.	
4	Reliable Computing Security	Processes and practices for safe and secure computing across the campus are routinely missing. When they do exist, they are poorly defined and often avoided.	1) Security mitigation now represents the largest portion of departmental IT administrator time and is the greatest contributor to downtime.	1) Develop a training program of relevant security requirements and guidelines. Require participation in this program for administrators of compromised machines by April 30, 2005. 2) 90% compliance with campus minimum security standards by June 30, 2006 3) Year-by-year measurable reduction in unplanned downtime and number of systems security incidents.	2a) Minimum security standards go into effect May 1, 2005. 2b) Most departments are working toward compliance with minimum standards 3) SNS is building a database to measure the number of security incidents	1) SNS and Cal Pact to develop a training program on security requirements and guidelines for administrators. 2) CISC to establish a policy on required attendance at administrator training. 3) Internal Audit and Computer Information Security Committee (CISC) to develop and plan for security audits. 4) Create an emergency operations and response plan for technology failures and significant security breaches.
5	Reliable Physical Environment for Information and Services	Many campus computing components, including servers, data storage, and network equipment are housed in substandard, insecure and inappropriate spaces such as custodial closets and utility closets.	1) Many departmental servers are housed in inappropriate locations. An example of this is: LSCR recently took over the computing operations in an L&S department. No one in the department even knew where the server was. It turned out to be a rack mountable server, without a rack, sitting underneath a bunch of papers in the department's library.	1) Develop and publish environmental standards for housing servers and data December 31, 2004. 2) 90% of campus servers should meet environmental standards by June 30, 2008.	1a) IST-CNS has published environmental standards for network electronics. These can be shared and applied to departmental servers. 1b) IST-CNS has written a draft standard for building out environmental spaces that can be shared between network equipment and departmental servers. 2a) The campus has a campus computing center that is available to all departments. 2b) Some departments have published standards requiring that servers reside in server rooms.	1) Review standards for network electronics and determine applicability to departmental servers. 2) Develop an audit cycle for departmental servers. 3) Acquire funding to remediate problems resulting from audits. 4) Improve central mail, web and file sharing services to reduce the need for departments to self-manage servers.