Today's Top Ten List for Internal Controls

1) Reconcile all budgets on a regular monthly basis. Make sure all transactions are valid, appropriate and supported. There should be evidence of review and evidence of oversight/monitoring by the chartstring owner. Make sure funds are used for their intended purpose!
2) Segregate duties so no one person handles the entire transaction process (cash, payables, etc.). There are "checks and balances" to ensure funds actually get deposited or disbursements appropriately.
3) Communicate – it's better to share concerns – it is expected that you will share concerns so that they can get addressed. Make sure all of your staff members are properly trained, know where to find (and are familiar with) NU policies and procedures, know where to go for help, and how to voice their concerns. Consider … your supervisor, your supervisor's supervisor, enterprise systems help desks, Dean's office contacts, central admin process owners, Audit & Advisory Services … the Ethics Point hotline.
4) Secure cash and checks in locked drawers or safe. Limit access to cash registers, drawers, and safes. Restrictively endorse checks upon receipt. Record every check in a log when received and make sure to reconcile to the deposit credit on your budget statement. Get deposits to the Bursar's Office in a timely fashion.
5) Purchasing – actively do competitive bidding. Question any "sole source" option. Scrutinize and authenticate the need for setting up new vendors.
6) P-cards – keep numbers confidential (do NOT share cards!). Keep documentation to support every transaction. Reconcile all p-card transactions quickly and thoroughly.
7) Practice safe computing … see: "Security Recommendations for Desktop Computers" found at http://www.it.northwestern.edu/policies/desktop_security.html
    a. Always choose a hard-to-guess password and never share it with anyone under any circumstances (don't write it down, give it over the phone, or tell it to a boss or co-worker).
    b. Don't click on links in e-mails to go to a website. If you need to visit a company's website, enter it directly into your browser.
    c. Encrypt your computer (PDAs and jump drives!), especially if it contains any confidential data (including, but not limited to student or faculty data, research data, or financial information.)
8) Secure your offices, workspaces, labs, computers, personal belongings. Remember all NU equipment is the property of the University. You should have no expectation of privacy with regard to what is stored on your PC/in your desk, etc. Personal files, photos, software, music are not appropriate to be stored on your work computer.
9) Be aware and conscientious of changes, unusual behaviors, strange activities, answers that don't make sense. Think about "risks" on a regular basis. How could fraud be perpetrated in your area? What key controls do you rely upon – and are they working? Consider how well risks are controlled and talk with someone if you feel issues could expose the University to a significant loss, damage or penalty if the risk were to occur.
10) Do not put your employees in a position where they can be suspected of wrongdoing because there are not adequate controls in place. Regularly solicit their input and provide adequate supervision.

Make "doing the right thing" always the easy choice through effective internal controls.