

RISK ASSESSMENT



Information Services' staff members conduct annual risk assessments to identify potential technology weaknesses and vulnerabilities. In addition, Information Services biennially commissions an external information security review of the College's Technology Support and Enterprise Systems policies, procedures and infrastructure. The review includes technical and functional policies and procedures, security in place, resistance to unauthorized penetrations, and a physical assessment of the facilities.

The last Information Services formal risk assessment listed eight medium risks. Based on the protocols of the Educause Center for Applied Research Methodology, *no serious risks were identified*. The following is a list of medium-risk items, in order of risk severity and likelihood:

- Failure of the College Web site.
- Loss or prolonged absence of key network, database administration, Web or programming personnel.
- Physical damage to server or telecommunications rooms caused by fire, flood, vandalism, building failure or a weather-related event.
- Major failure of the Cisco 6500 main core router.
- Theft or loss of a computer, hard drive, backup tape or other storage media that contains sensitive information.
- Major failure of essential data systems.
- Extended power outage on all or part of the campus.
- Failure of the data tape backup system.

Since this assessment, Information Services has reduced, or has made recommendations about reducing, the risk for each of these items. KPMG, the College's financial auditing firm, also reviews IS infrastructure, policies and procedures. The latest review complimented IS on its environment and operations.

THREE THINGS YOU SHOULD KNOW ABOUT RISK ASSESSMENT:

- IS formally reviews its operations and environment annually to identify and evaluate risks.
- A biennial external review of information security practices was completed in June 2013. No serious issues were identified.
- IS makes mitigation of risk its top priority and uses its internal operating budget to mitigate risk if possible.

For more information, contact Bruce Carpenter, Director of Technical Support and Information Security Officer, at x5242 or bwcar@conncoll.edu.