

Information Security Risk ASSESSMENT

Given today's dynamic Internet environment and emerging networking technologies, Community Colleges must maintain comprehensive, proactive and compliant safeguards of critical educational assets.

An ongoing risk assessment program is vital to assuring a sound information technology security program. This is paramount for maintaining a college's educational mission.

A formal risk assessment process should be the point at which college leadership and information technology professionals come together. While senior administrators must focus on meeting the educational and support needs of students, faculty and staff, IT professionals must keep campus network academic and administrative applications operational, safe and secure. A comprehensive risk assessment can help both groups understand the risks of operating a community college with ineffective or inappropriate security controls.

Secure Enterprise Computing will work with key college staff, both technical and non-technical, to assess your organization's network and application security and IT policies and procedures. The result of this review is written recommendations for improving your overall IT security posture.

The main objectives of the assessment include:

- How effectively the college is maintaining security, integrity and confidentiality of critical school IT assets.
- How the college is protecting against anticipated, reasonable threats or hazards.
- How well the college is protecting against unauthorized access to information.
- How the college has documented its policies and procedures in conformity to relevant state and federal rules and laws.
- How the college is using accepted IT project management practices to add or upgrade existing IT resources.

Assessment Methodology - Our experienced security engineers will use information gathered through a series of interviews, software

tools, and our own industry experience and understanding of industry best practices and standards such as the Code of Practice for Information Security Management (ISO 17799), the NIST Special Publication 800-42 and the FBI/SANS Top 20 Vulnerability List to assess the state of your network.

The evaluation focuses on the following areas:

- Business continuity
- System access control
- System development and maintenance
- Physical and environmental security
- Compliance
- Personnel security
- Organizational security
- Operations and change management
- Policy.

This assessment measures and analyzes an organization's susceptibility to outside threats by verifying the integrity of the existing security controls. Our assessment methodology also identifies vulnerabilities within the campus, advises on the risk and provides prioritized recommendations, allowing you to effectively secure operations in today's dynamic environment.

At the end of this assessment, college management will be provided with:

- An appreciation of the threats to assets.
- An articulation of vulnerabilities and weaknesses.
- A strategy for prioritized remediation.

Our goal is to allow both senior management and information security staff the ability to understand the real risks faced by the organization.