



Cyber Audit-Talon Cyber Tec

Board of Trustee Retreat - April 20, 2012

Tier 1 Cyber Security Audit

- Quick high-level evaluation of the core aspects of an organization's network environment and technology infrastructure to determine where deficiencies may exist.
- Readiness survey that balances operational requirements against security needs:
 - reduce risks

Tier 1 Cyber Security Audit

- Neutralize threats
- Evaluate network environment & technology infrastructure
 - ✓ Security policies and procedures
 - ✓ Security organization and personnel
 - ✓ Security access control & protection mechanisms
 - ✓ Security incident
 - ✓ Business continuity management
 - ✓ Security compliance

Tier 2 Cyber Security Audit

Builds upon the baselines established during the Tier 1 audit. A more extensive audit to comprehensively evaluate all technical and administrative security vulnerabilities that can be leveraged to attack critical data and information systems.

- Internal and external evaluation of the network environment
 - What needs to be protected

Tier 2 Cyber Security Audit

- Why is it at risk?
- Isolating threats and vulnerabilities
- Solutions to mitigate risks

The Cyber security audits do not entail drafting security policies or implementing recommendations to mitigate security issues. They also do not include application and source code reviews, computer forensics, and training.

Questions?

