

# TEK TEAM XTREME

## **Business/Technology ASSESSMENT:**

The Assessment is our first contact point with a Dr. to help him/her understand the business risks posed by his/her current technology implementation. The Assessment is analogous to a patient check-up, allowing the “Patients” general level of health to be assessed. The Assessment comes in two parts:

**Data Collection** – is the information-gathering portion, where we collect information about the Dr.’s technology implementation, and research any business risks:

- 1) Detailed mapping of the current technology implementation
- 2) Detailed mapping of all processes and procedures used to manage the current technology implementation
- 3) Risks associated with external intrusion/data theft
- 4) Risks associated with internal intrusion/data theft
- 5) Risks associated with tracking tools and software used by the business
- 6) Risks associated with tracking and protecting usernames, passwords, licenses, etc.
- 7) Risks associated with the integrity of critical data
- 8) Risks associated with the availability of critical data
- 9) Risks associated with the availability of technology components (as well as identifying outdated hardware and software)
- 10) Identification of single points of failure in the current technology implementation

**Reporting** – is the layout in terms the Dr. can understand, of the information gathered in the 1<sup>st</sup> step, plus methods for lowering any risks uncovered:

- 1) Documented Maps of the technology implementation, and processes and procedures used to manage it.
- 2) Documenting all Technology specifics: Software ID’s, Keys, Hardware Serial #’s, Etc.
- 3) Documenting the risks uncovered in each area of the assessment and explained in language understandable by the Dr., and/or his/her staff (Business Risk Assessment).
- 4) Documenting method(s) for lowering or eliminating any and all risks that have been identified, for each area:
  - a. Including backup plans for critical technology component repair or replacement.
  - b. Explanation of processes and procedures that could be implemented to track or manage various assets.
  - c. Proposed configuration changes or enhancements that could improve security/reliability/dependability of the existing implementation.
  - d. Etc.

**Benefits** – there a number of benefits to having an assessment, even if you are already working with a technical “guru”. These include:

- 1) You have a map of the technology that you rely on, and all licenses that we could locate, in one place in case of an emergency. This information is understandable and usable by you, your staff, or your technical guru.
- 2) You have an independent assessment of key technology-related risks to your practice.
- 3) You have an understanding of how to lower your exposure to costly system failure, hacking, data theft and loss, and viruses that can destroy important data.
- 4) You have a plan for managing most technology-related emergencies and recovering as quickly as possible.
- 5) You have a basic roadmap to making your office and practice both safe and paperless.