Section 7:
How important is your information?

Records and data are not all equally valuable. Therefore, not all information systems containing records will require the same security measures and levels of trustworthiness. In determining the importance of your information, you may want to consider such things as:

- What laws and regulations apply to your data?
- What are your industry's standards for system security, data security, and records retention?
- What areas and records might lawyers and auditors target?
- What data is of permanent and/or historical value to you and to others?

Certain policy mandates, such as the Minnesota Data Practices Act and others concerned with records management (refer to Appendix D), determine the precise value and security level of some information. These laws are written without respect to media or format. At present, however, there are no widely applicable models available for managing electronic records like there are for paper. The ever-increasing use of electronic records forces us to look at new ways to actually answer policy demands while efficiently using government resources.

Agencies should have some leeway to decide the significance of their records, their functional priorities, and the resources available to them as a basis for making informed choices about the appropriate practices to apply. The criteria set will help government agencies manage the risks associated with their information systems. While comprehensive in scope, the set will not apply to all systems equally. A system holding purchase orders, for example, will not have as high a legal profile and need for security and trustworthiness as one containing confidential medical information.

You must show that you have made informed choices that are appropriate for your records and that you have appropriate policies and procedures in place that are followed during the routine course of business—you are accountable for your actions. Lawyers and auditors, for instance, may examine your information systems in minute detail, looking for things like undocumented delays, variances from established procedures, and holes in your security in terms of access to your system and your records (refer to Appendix E for case laws regarding electronic records and to the Legal Risk Analysis Tool in Appendix G for additional assistance). These inquiries can be answered with documentation showing that you have examined your systems and have made informed decisions concerning the handling of your records.

So, you see, the criteria set is really a tool for risk management!