**EXCERPT from**

**The National Institute of Standards and Technology HIPAA Security Rule Toolkit User Guide**

**How to Approach Questions**

Most of the questions in the Toolkit can be answered by one of three choices:

Yes

No

Not Applicable

Selecting either Yes or No is neither inherently correct nor incorrect. The answer truly depends

upon the size, implementation, and manner of justification provided by the respondent. Why is

this important? Consider the case studies below.

Case Study #1

In the following example, the question involves a number of elements to be addressed in an

organizations’ risk assessment policy.



It may be that an organization has addressed some but not all of these elements in its risk

assessment policy documentation. If *training* and *compliance* were not addressed in the

documentation, should the user select the No option?

Not necessarily.

This will be a subjective evaluation after the pertinent documentation has been examined. The

user may feel that all elements of the question have been addressed and therefore feels

justified in selecting the Yes option. This can be true for any size organization. In either case, it

is suggested that the user make liberal use of the comments box. In this case, it is valid to

choose either Yes or No.

Case Study #2

In the following example, the user is asked to supply an answer and supporting information to

justify that answer.



In both situations, the user is requested to document supplemental information in the comment

field. In many instances, the user is encouraged to make extensive use of the comment field to

provide additional information, reference internal documents, or add simple notes on a topic to

refer to later. Depending upon the manner in which an organization wishes to use the Toolkit,

the comments field can hold internal notes and detailed descriptions as to why a requirement

was or was not addressed.