

Information Technology Security Council

Frequently Asked Questions and Answers about the IT Security Self-Assessment (note these do not apply to Regents Institutions who use a different assessment)

Q1: What applications are we to use to answer the questionnaire?

A1: Pick one application that you would rate mission critical, i.e. you need the application running within 48 hours of any contingency, or else answer in general for your agency across all applications.

Q2: How do I answer the question "Are boundary controls effective?"

A2: First determine what boundary controls you employ, e.g. IDS, Antivirus, etc. and then determine if they stop the threats to penetrate your application.

Q3: What does "Connected Systems" mean?

A3: It means any application system that is interconnected via a software application to your application you are evaluating.

Q4: What do the various ratings in Column B represent?

A4: The ratings represent the level of sophistication that the agency has for the given question. A "0" rating means "We do not do at all", a "1" rating means that "We have an Informal Practice Only", a "2" rating means "We have written Policy or Procedures", a "3" rating means "We have Written Policy and Procedures Implemented", a "4" rating means "We have Written Procedures that are Reviewed and Tested on a regular basis", and finally a "na" means "It is not applicable for us." Just rate your agency from "0" to "4" for the highest level that the agency has implemented for each particular question. Note that the "na" should not be used as a substitute for a "0". For example, if your agency does not have a contingency plan at all, you should rate your agency as a zero on question CP-2.1. However, if you agency does not use VOIP, you would use a "na" on questions SC-19.1 through SC-19.

Q5: Is one person expected to complete the entire survey?

A5: Depending on the size of the agency and the given application being evaluated, one person may or may be not knowledgeable to complete all sections of the survey. That is why the column for initials is there. If you want to subdivide the questionnaire and have different people be responsible for different sections, the respondents can indicate their initials in the last column. That way, if any follow through is necessary, you know who responded to a given question.

Q6: How will you score my survey if I leave a question blank?

A6: To avoid any confusion on our part, or to avoid having your survey scored incorrectly, please try to answer every question or indicate that it's not applicable. However, if you do leave something blank here's what we'll do:

If you leave a question blank, we will score it as a "0." In other words we'll assume you don't have a practice or a policy for that area.

Q7: In some of the sections, there appears to be some missing numbers. Are some questions missing from my copy?

A7: No. The assessment is tailored for the Moderate level as defined by NIST. These are some gaps in the numbers for controls that don't apply at the Moderate Level. For example, the questions go from AC-2.6 to AC 2-9.. Control questions AC-2.7 and AC-2.8 only apply to the High Level and hence are omitted.

Q8: What am I supposed to use the "Comments" section for?

A8: We encourage citations and exact locations of policies and procedures each year to be included in this column, "C" . The paper copies of the IT Security Self-Assessment should be saved and used for reevaluation and reuse during the next evaluation period.