

PEPS RA Evaluation

As I mentioned earlier, final decisions for acceptance of the risk assessment results are up to you. Having said that, I looked at Spectrum's responses and the proposed countermeasures they added/changed seem to look fine. I am concerned, however, by the statements in the opening paragraph. First of all, if possible they should propose as many possible countermeasures that may fix the vulnerability as possible. It is your job, along with your system manager, to determine which (if any) of the proposed countermeasures you wish to actually implement (remember the Security Plan training?). I may be mistaken, but it sounded like Spectrum was saying they were only going to add the changes regarding the security banner. I would recommend asking the assessors to include all proposed countermeasures so that you have the full range of options to choose from (or even add to if you have other possible corrective actions).

Second, I disagree with their recommendation regarding not updating the 1998 Security Plan. You are required to update your security plan after any major changes or at least every three years; with the way systems get upgraded around here, most likely any security plan not updated yearly would be out of date. I understand that sections of PEPS may be stripped to another system, but 1) you have a severely out of date security plan, and 2) just because the current project plan says that PEPS will be changed, that doesn't mean the project plan itself might not get changed later. Again, the final decision is up to you, but my recommendation is to look into updating.