CASE STUDY: REVIEWING AN ASSESSMENT REPORTING TEMPLATE (UNIT 5):

OVERVIEW:

Instructions: You are tasked with reviewing the assessment template from PurpleSec.

Answer the following questions:

Does this template meet the NCSC stated requirement of preparing a baseline to use as a reference point for pen tests? If not what changes/amendments would you make?

What are the two best lessons/examples presented in the report?

What two things do you think are unnecessary or could be done more effectively?

According to NCSC (2022), a pen test report should include:

Any security issues uncovered

An assessment by the test team as to the level of risk that each vulnerability exposes the organisation or system to

A method of resolving each issue found

An opinion on the accuracy of your organisation's vulnerability assessment

Advice on how to improve your internal vulnerability assessment process

Answer:

Reading the assessment template from PurpleSec I can see that it was designed well. The document has illustrated and identified many vulnerabilities and has categories it in multiple tables. The document contains three tables which identifies low risk, medium risk, and high risk vulnerabilities. Each table listed the name of the vulnerability, a description of it, a solution to it, and the total count of it. The table is presented in a fairly easy way to understand however it is a little on the technical side. The table could have been modified to demonstrate those vulnerability in a none technical manager to help non-technical people understand these issues and how to fix them. Furthermore the document illustrated the testing methodology and finding which is great way of knowing how was the test conducted and what the tests reveal.

In the end, the document has added the a recommendation section on how to fix the above vulnerabilities, however, it is very technical. In addition the document also included security policies to be implemented. Overall the report was great, it could have used the STRIDE and DREAD model to represent the data and it could have included a less technical section.