

1. An organization is considering developing an encryption policy in its organization. The penetration tester from the team starts documenting specific products and configurations to put into the policy. Should the policy contain these details?

If I were to apply the core principles in this situation, the policy should not contain specific products and configurations in detail. Instead, it should outline the organization's approach to encryption, and how encryption effectiveness will be monitored and updated.

2. An organization is considering placing all its policies, procedures, standards, and guidance in a single handbook so executive management must sign off only once. What are the advantages and disadvantages to this approach?

The advantage of this approach is that it will make the signing of the handbook faster because the executive manager only needs to sign once, however it would not be practical as each section should be separated to create a plan that is organized and allows for easy updates without causing problems in the plan.