If an organization has three information assets to evaluate for risk management, as shown in the accompanying data, which vulnerability should be evaluated for additional controls first? Which one should be evaluated last?

Data for Exercise 1:

Switch L47 connects a network to the Internet. It has two vulnerabilities: it is susceptible to hardware failure at a likelihood of 0.2, and it is subject to an SNMP buffer overflow attack at a likelihood of 0.1. This switch has an impact rating of 90 and has no current controls in place. You are 70 percent certain of the assumptions and data.

Server WebSrv6 hosts a company Web site and performs e-commerce transactions. It has a Web server version that can be attacked by sending it invalid Unicode values.

The likelihood of that attack is estimated at 0.1. The server has been assigned an impact value of 100, and a control has been implanted that reduces the impact of the vulnerability by 75 percent. You are 80 percent certain of the assumptions and data.

Operators use an MGMT45 control console to monitor operations in the server room. It has no passwords and is susceptible to unlogged misuse by the operators. Estimates show the likelihood of misuse is 0.1. There are no controls in place on this asset; it has an impact rating of 5. You are 90 percent certain of the assumptions and data