Summary Vendors play a crucial role in modern IT environments, particularly when organizations make significant use of cloud service providers. In this chapter, you learned how organizations develop and maintain enterprise risk management (ERM) programs to manage these risks and adopt strategies of risk mitigation, risk transference, risk avoidance, and risk acceptance to maintain a risk profile that is consistent with the organization's risk appetite. **Exam Essentials Policy frameworks consist of policies, standards, procedures, and guidelines.** Policies are high-level statements of management intent for the information security program. Standards describe the detailed implementation requirements for policy. Procedures offer step-by-step instructions for carrying out security activities. Compliance with policies, standards, and procedures is mandatory. Guidelines offer optional advice that complements other elements of the policy framework. **Organizations often adopt a set of security policies covering different areas of their security programs.** Common policies used in security programs include an information security policy, an acceptable use policy, a data ownership policy, a data retention policy, an account management policy, and a password policy. The specific policies adopted by any organization will depend on that organization's culture and business needs. **Policy documents should include exception processes.** Exception processes should outline the information required to receive an exception to security policy and the approval authority for each exception. The process should also describe the requirements for compensating controls that mitigate risks associated with approved security policy exceptions. **Know how risk identification and assessment helps organizations prioritize cybersecurity efforts.** Cybersecurity analysts try to identify all of the risks facing their organization and then conduct a business impact analysis to assess the potential degree of risk based on the probability that it will occur and the magnitude of the potential effect on the organization. This work allows security professionals to prioritize risks and communicate risk factors to others in the organization. **Know that vendors are a source of external risk.** Organizations should conduct their own systems assessments as part of their risk assessment practices, but they should conduct supply chain assessments as well. Performing vendor due diligence reduces the likelihood that a previously unidentified risk at a vendor will negatively impact the organization. Hardware source authenticity techniques verify that hardware was not tampered with after leaving the vendor's premises. **Be familiar with the risk management strategies that organizations may adopt.** Risk avoidance strategies change business practices to eliminate a risk. Risk mitigation techniques reduce the probability or magnitude of a risk. Risk transference approaches move some of the risk to a third party. Risk acceptance acknowledges the risk and normal business operations are continued despite the presence of the risk.