Risk management is the process of identifying risk, as represented by vulnerabilities, to an organization’s information assets and infrastructure, and taking steps to reduce this risk to an acceptable level. Each of the three elements in the C.I.A. triangle is an essential part of every IT organization’s ability to sustain long-term competitiveness. When an organization depends on IT-based systems to remain viable, information security and the discipline of risk management must become an integral part of the economic basis for making business decisions. These decisions are based on trade-offs between the costs of applying information systems controls and the benefits realized from the operation of secured, available systems.

Risk management involves three major undertakings: risk identification, risk assessment, and risk control. Risk identification is the examination and documentation of the security posture of an organization’s information technology and the risks it faces. Risk assessment is the determination of the extent to which the organization’s information assets are exposed or at risk. Risk control is the application of controls to reduce the risks to an organization’s data and information systems. The various components of risk management and their relationship to each other are shown in Figure.

Risk Identification

A risk management strategy requires that information security professionals know their organizations’ information assets—that is, identify, classify, and prioritize them. Once the organizational assets have been identified, a threat assessment process identifies and quantifies the risks facing each asset.

Risk Assessment

Now that you have identified the organization’s information assets and the threats and vulnerabilities, you can evaluate the relative risk for each of the vulnerabilities. This process is called risk assessment. Risk assessment assigns a risk rating or score to each information asset. While this number does not mean anything in absolute terms, it is useful in gauging the relative risk to each vulnerable information asset and facilitates the development of comparative ratings later in the risk control process.

Risk Control Strategies

When organizational management determines that risks from information security threats are creating a competitive disadvantage, they empower the information technology and information security communities of interest to control the risks. Once the project team for information security development has created the ranked vulnerability worksheet, the team must choose one of five basic strategies to control each of the risks that result from these vulnerabilities. The five strategies are defend, transfer, mitigate, accept, and terminate

