Security gaps occur whenever there are lapses in the secure application or implementation of a company’s policies, protocols, procedures, and practices. Risk management helps shrink the security gap by identifying, assessing, prioritizing, and addressing various forms of risk. The difference between established security controls and controls needed to address all vulnerabilities is called the **security gap**.

There are several reasons for security gaps including the following:

* Unintentional lack of security policy or procedure for a certain vulnerability
* Intentional and willful neglect of security policy or procedure
* Unintended consequence of recent IT infrastructure change
* Result of changes to external requirements, such as laws, regulations, and practices

The two primary goals of risk management include:

* Minimize the effects of negative risks that occur.
* Maximize the effects of positive risks that occur.

Risk equals the number of threats against an organization’s resources multiplied by the number of vulnerabilities. Threat is the likelihood that a bad event will occur, vulnerability is the potential weak point, and risk is the result of threat and vulnerability combined.

Risk mitigation is the process of investing secure measures for reducing risk over time. Problem severity refers to how badly and broadly a problem can affect critical resources and the nature of the problem. A system intrusion may have greater severity if it involves disclosure of confidential information and less severity if the intruder gained no special privileges and modified no important data.

Risk management is the process of identifying, analyzing, planning, and responding to risks. Threats and vulnerabilities are permanent fixtures of any IT organization and must be monitored and managed over time. As a result, risk management is a recurring process that seeks to constantly re-evaluate the security stance, particularly with regard to emerging threats and attack trends.

Companies should take a proactive approach to risk management. Risk management is an ongoing process in maintaining IT infrastructure that requires consistent monitoring and careful observation.

Not all risk is bad and some risk is unavoidable. Therefore, there are acceptable levels of risk and liability. When you cannot avoid local natural disasters, for example, that is an acceptable form of risk. You cannot avoid hardware failure, which is acceptable risk that isn’t intentionally harmful. Certain forms of risk are avoidable, preventable, and intolerable, such as using company resources to violate company security policies by accessing privileged systems or resources from a legitimate user account.