3.1.5 Security Management Facts

Security management is the overall security vision for an organization as well as the ongoing implementation and maintenance of security. The goal is to preserve the confidentiality, integrity, and availability of all critical and valuable assets. Senior management is responsible for security management. Senior management defines the corporate security posture or tone (the organization's outlook and approach to security) and provides funding for the security program.

Under the direction of senior management, security professionals establish specific policies and plans related to the organization's security implementation. In addition to protecting company assets and employees' personal information, these plans and policies safeguard the organization from liability and exposure. Plans and policies are most effective if the following steps are implemented in their execution:

1. Assess the risk
2. Create a policy
3. Implement the policy
4. Train the organization on the policy
5. Audit the plan to make sure it is working

One of the best ways to implement operational security is to apply the concept of defense in depth. *Defense in depth* is the premise that no single layer is completely effective in securing the organization. The most secure system has many layers of security, eliminating single points of failure. The following table identifies the four components of operational security that help to establish defense in depth:

Component	Areas of Focus
Change Control	*Change control* regulates changes to policies and practices that could impact security. The primary purpose of change control is to prevent unchecked change that could introduce reductions in security. Change control must be a formal, fully documented process. The following are the change control process steps: 1. Identify the need for a change and submit it for approval. 2. Conduct a feasibility analysis, including technical and budgetary considerations. 3. Design the method for implementing the change. 4. Implement the change. 5. Test the implementation to make sure it conforms to the plan and that the change does not adversely affect confidentiality, integrity, and accessibility. 6. Document the change. 7. Analyze feedback. In the event that a change unintentionally diminishes security, an effective change control process includes rollback. A *rollback* makes it possible to revert the system back to the state it was in before the change was put into effect.
Employee Management	*Employee management* reduces asset vulnerability from employees by implementing processes that include the following: - Pre-employment processing - Employee agreement documents - Employee monitoring - Termination procedures
Security Awareness	*Security awareness* is designed to: - Familiarize employees with the security policy - Communicate standards, procedures, and baselines that apply to an employee's job - Facilitate employee ownership and recognition of security responsibilities - Establish reporting procedures for suspected security violations - Follow up and gather training metrics to validate: - Employee compliance - The organization's security posture
Physical Security	*Physical security* is the protection of assets from physical threats. Physical security procedures include the following: - Choosing a secure site and securing the facility - Protecting both data and equipment from theft, destruction, or compromise - Implementing environmental and safety measures to protect personnel and the facility - Disposing of sensitive material that is no longer needed