Quiz 5

Most large software systems do not have security weaknesses. **False**

**Texts, Online resources, and Specific system hardening guides** are resources that should be used as part of the system security planning process.

**White listing** applications is a control that limits the programs that can execute on the system to just those in an explicit list.

A plan needs to identify appropriate personnel to install and manage the system, noting any training needed. **True**

A very common configuration fault seen with Web and file transfer servers is for all the files supplied by the service to be owned by the same “user” account that the server executes as. **True**

The **archive** process retains copies of data over extended periods of time in order to meet legal and operational requirements.

IT security needs to be a key part of an organizations overall management plan. **True**

IT security management has evolved considerably over the last few decades due to the rise in risks to networked systems. **True**

IT security management consists of first determining a clear view of an organization IT security objectives and general risk profile. **True**

Because the responsibility for IT security is shared across the organization, there is a risk of inconsistent implementation of security and a loss of central monitoring and control. **True**

Once the IT management process is in place and working the process never needs to repeated. **False**

The **ISO** has revised and consolidated a number of national and international standards into a consensus of best practice.

**IT security management** ensures that critical assets are sufficiently protected in a cost-effective manner.

The implementation phase comprises not only the direct implementation of the controls, but also the associated training and general security awareness programs for the organization. **True**

Detection and recovery controls provide a means to restore lost computing resources. **True**

The selection of recommended controls is not guided by legal requirements. **False**

**Detection and recovery** controls focus on the response to a security breach, by warning of violations or attempted violations of security policies.

Management controls refer to issues that management needs to address. **True**

Operational controls range from simple to complex measures that work together to secure critical and sensitive data, information, and IT systems functions. **False**

Periodically reviewing controls to verify that they still function as intended, upgrading controls when new requirements are discovered, ensuring that changes to systems do not adversely affect the controls, and ensuring new threats or vulnerabilities have not become known are all **security compliance** tasks.