ISO 17799

Rajesh Muley

Introduction

ISO 17799 is an internationally recognized Information Security Management Standard

suitably protect this asset in order to ensure business continuity, minimize business damage, and maximize return on investments.

Benefits of ISO 17799

ISO 17799 offers a benchmark against which to build organizational information security. It also offers a mechanism to manage the information security process.

- An internationally recognized, structured methodology
- A defined process to evaluate, implement, maintain, and manage information security
- A set of tailored policies, standards, procedures, and guidelines
- Certification allows organizations to demonstrate their own and evaluate their trading partners' information security status

Controls

◇**Security policy:** Adopting a security process that outlines an organization's expectations for security, which can then demonstrate management's support and commitment to security.

◇**Security organization:** Having a management structure for security, including appointing security coordinators, delegating security management responsibilities and establishing a security incident response process.

◇**Asset classification and control:** Conducting a detailed assessment and inventory of an organization's information infrastructure and information assets to determine an appropriate level of security.

Controls

◇**Personnel security:** Making security a key component of the human resources and business operations. This includes writing security expectations in job responsibilities (IT admins and end users), screening new personnel for criminal histories, using confidentiality agreements when dealing with sensitive information and having a reporting process for security incidents.

◇**Physical and environmental security:** Establishing a policy that protects the IT infrastructure, physical plant and employees. This includes controlling building access, having backup power supplies, performing routine equipment maintenance and securing off-site equipment.

◇**Communications and operations management:** Preventing security incidents by implementing preventive measures, such as using antivirus protection, maintaining and monitoring logs, securing remote connections and having incident response procedures.

Controls

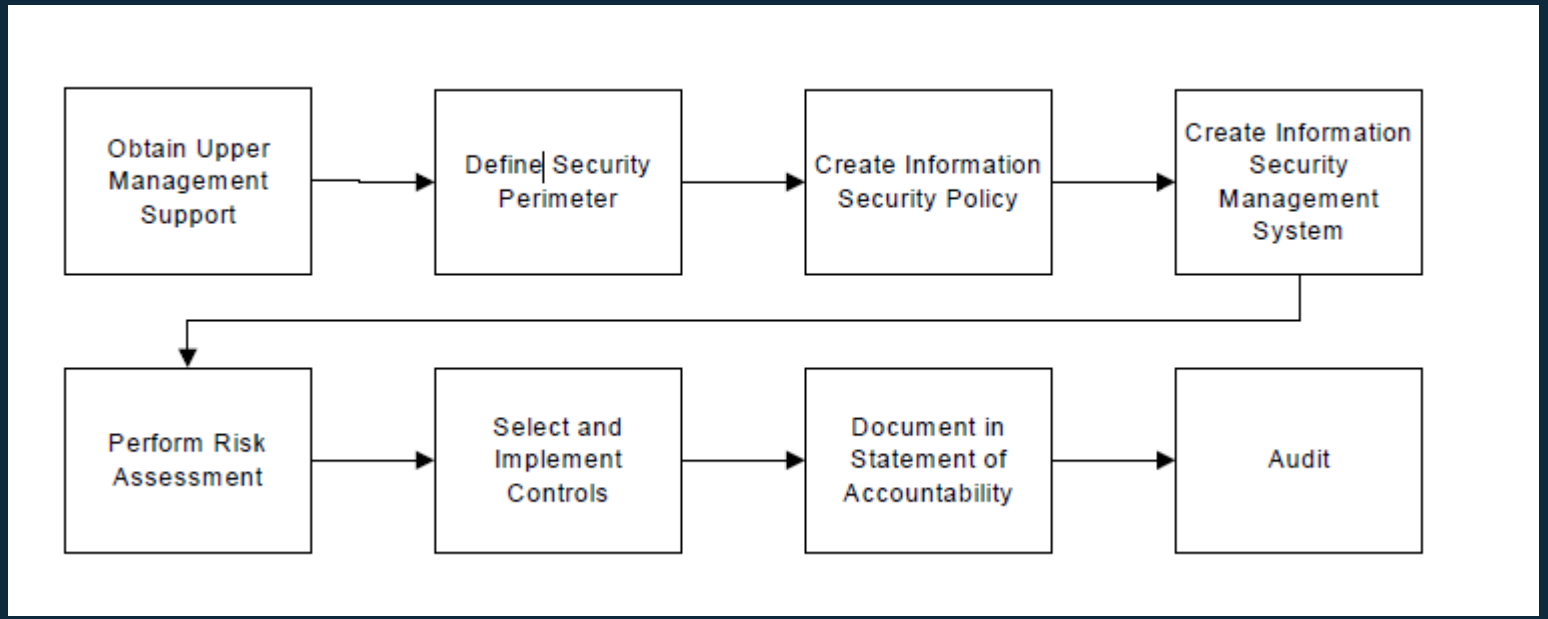
◇**Access control:** Protecting against internal abuses and external intrusions by controlling access to network and application resources through such measures as password management, authentication and event logging.

◇**Systems development and maintenance:** Ensuring that security is an integral part of any network deployment or expansion, and that existing systems are properly maintained.

◇**Business continuity management:** Organization’s ability to counteract the interruptions to normal operations. Planning testing and maintenance

◇**Compliance:** Complying with any applicable regulatory and legal requirements, such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA).

Process for implementing information security management using ISO 17799



Security Policy Statement

- Confidentiality of information will be assured
- Integrity of information will be maintained
- Availability of information to authorized users will be met.
- Regulatory and legislative requirements will be fulfilled
- Information security training will be available to all staff
- Breaches of information security, actual or suspected, will be reported to, and investigated by the Information System Security Officer.

Information Security Management System

- Security Structure Organization Chart
- Risk Management Strategy
- Information System Security Officer job description
- Management Security Forum charter
- ISMS Document Control Plan
- Security Risk Assessment
- Statement of Applicability
- Customer Code of Conduct


thanks