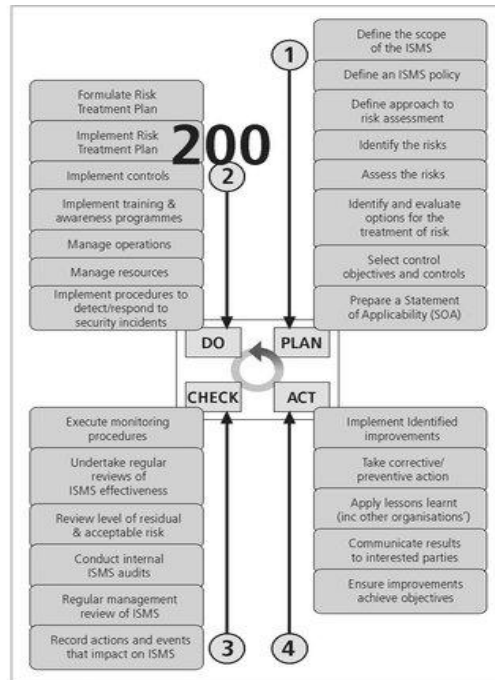


CONTENT OUTLINE

The Sections of ISO/IEC 17799

- 1) Organizational Security Policy
 - 2) Organizational Security Infrastructure
 - 3) Asset Classification and Control.
 - 4) Personnel Security
 - 5) Physical and Environmental Security
 - 6) Communications and Operations Management
 - 7) System Access Control
 - 8) System Development and Maintenance.
 - 9) Business Continuity Planning
 - 10) Compliance
- The stated purpose of ISO/IEC 17799 is to ~~give~~ give recommendations for information security management for use by those who are responsible for initiating, implementing, or maintaining security in their organization.
 - It is intended to provide a common basis for developing organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings.
 - This International Standard is actually drawn from only the first volume of the two-volume British Standard 7799.
 - Volume 2 of BS7799 picks up where ISO/IEC 17799 leaves off.
 - Where Volume 1 of BS7799 and ISO/IEC 17799 are focused on a broad overview of the various areas of security, providing information on 127 controls over ten broad areas.
 - Volume 2 of BS7799 provides information on how to implement Volume 1 and ISO/IEC 17799 and how to set up an information security management system (ISMS).



Courtesy of Gamma Secure Systems

FIGURE 6-10 BS7799:2 Major Process Steps¹⁰

- Several countries have not adopted 17799 claiming there are fundamental problems:
 - The global information security community has not defined any justification for a code of practice as identified in the ISO/IEC 17799
 - 17799 lacks “the necessary measurement precision of a technical standard”
 - There is no reason to believe that 17799 is more useful than any other approach currently available
 - 17799 is not as complete as other frameworks available
 - 17799 is perceived to have been hurriedly prepared given the tremendous impact its adoption could have on industry information security control
- Organizational Security Policy is needed to provide management direction and support