

INTRODUCTION TO ISO 17799

Information is one of the most valuable and essential assets for business survival and may be present in various forms: paper, electronic, mail, oral and audio-visual. Therefore, information management is increasingly vital for competitive success for all sectors of the economy. The purpose of information management is to safeguard the confidentiality, integrity and availability of information. Growing fraud, espionage, virus, and hackers have threatened the business information management because of the increased exposure and less control through modern information technology. Consequently, increasing expectations from business managers, partners, auditors, regulators, and other stakeholders demand for effective information management to ensure information sharing for business continuity and minimise business damage by preventing and minimising the impact of security incidents.

In 1995, British Standards Institute (BSI) launched the first standard regarding to information management in the world: “BS 7799 (Part One): Code of Practice for Information Security Management”. Based on the fundamental infrastructure of BS 7799, ISO (International Organization of Standardization) introduced the ISO 17799 standard regarding to the information management on December 1, 2000. The requirements of ISO 17799 standard includes: information security policy document, allocation of information security responsibilities, provide all users with education and training in information security, develop a system for the reporting of security incidents, introduce virus controls, develop a business continuity plan, control the copying of proprietary software, safeguard organizational records, follow the requirements for data protection, and establish procedures for complying with the security policy. The ten control sections of ISO 17799 standard includes: security policy, security organisation, assets classification and control, personnel security, physical and environmental control, development and computer network and management, system access control, systems maintenance, business continuity planning, and compliance.