This document provides guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27001 and is designed to avoid the satisfactory implementation of information security based on a risk management approach. Knowledge of the concepts, models, processes and technologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of this document. This document is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which wish to manage risks that can compromise the organization’s information security.

Information is crucial for the continuity and proper functioning of all individual organizations and the economies they fuel. This information must be protected against abuse by opportunistic people, protected against accidental or malicious modification or destruction and made available when it is needed. The ISO Information Security Management (ISO/IEC 27001) certificate provides assurance that the Information Security Management System (ISMS) has been implemented and is continuously improved to meet the organization’s information security needs.

The new edition of a bestseller, Information Technology Control and Audit, Fourth Edition provides a comprehensive guide to the information technology control and audit field. The fourth edition is a major update to the first edition, with new content on cloud computing, security controls and frameworks, and internal auditing. The book also includes updated information on the COBIT, ITIL, and ISO standards. This book is the leading guide for IT auditors and information technology managers, providing a comprehensive overview of the key concepts and practices.