

Complete BS7799/ISO17799 Documentation Toolkit

Complete BS7799/ISO17799 Documentation Toolkit

For less than the cost of one day of a consultant's time, the complete toolkit gives you:

- A model, pre-written Information Security Policy, Statement of Applicability and Information Security Manual (approximately 50 pages)
- An encapsulation of all the detailed BS7799/ISO17799 knowledge and experience of the IT Governance consultancy team
- Approximately 110 different pre-written documents, totalling nearly 400 pages
- No software to install – easy-to-use toolkit on standard MS Word
- The unique itGovernance documentation support service, giving you guidance on issues of adaptation, customisation and understanding, as and when they arise, simplifying and supporting your progress throughout the project
- Our 12 month automatic update service ensures that you automatically benefit from any improvements to the toolkit.
- "The **itGovernance Documentation Toolkit** is a unique blend of an outstanding, practical and comprehensive suite of pre-written document templates and value adding services that will **save you months of work** and get your BS7799/ISO17799 project off to a flying start. " Alan Calder, author of "[IT Governance: a Manager's Guide to Information Security and BS7799/ISO17799](#)".

CONTENTS LIST

1. Introduction and user guidance for the **BS7799/ISO17799 Documentation Toolkit**
2. PDCA process
3. Blank templates:
 - a. Policy, procedure, work instructions, meeting agenda, meeting minutes, schedule, checklist
4. Blank SLA template with detailed guidance on completion
5. Documentation Implementation Manager, to control the documentation project and manage all its micro-elements to a successful conclusion.
6. Features throughout the model documents:
 - a. Comprehensive coverage of the requirements of every clause of both standards
 - b. Clause-by-clause cross-referencing to both BS7799 and ISO 17799
 - c. Internal cross-referencing (because many individual procedures deliver compliance with more than one clause of the standard, or have to be interoperable)
 - d. Version-control in line with ISO version control requirements
 - e. Status control – enforcing "uncontrolled" status for print offs
 - f. Detailed, step-by-step guidance on how to use the model documents – including internal comments, footnotes and guidance.
 - g. Simple to use – entirely Microsoft Word based.
 - h. Early BS7799:2005 and ISO17799:2005 compliance.
 - i. Designed to be customized and adapted for your organization and your legal jurisdiction.

Complete BS7799/ISO17799 Documentation Toolkit

- j. Designed to be capable of integration with existing risk and quality management frameworks inside your organization

BS7799/ISO17799 MODEL DOCUMENTS CONTAINED IN THE TOOLKIT

- 7. Information Security Policy
- 8. Statement of Applicability
- 9. ISMS Manual
- 10. Business continuity plan (section 14 of ISO17799:2005)
- 11. Section 2 (of the Information Security Manual and of ISO17799:2005)
 - a. Document control procedure
 - b. Control of records procedure
- 12. Section 3
 - a. Agendas for two management meeting to initiate and to establish the ISMS
 - b. Draft minutes of two management meeting that initiate the project and establish the ISMS and approve the risk management framework
- 13. Section 4
 - a. Risk assessment tool (DOC 4.2)
 - b. Risk management framework (DOC 4.3)
 - c. Risk assessment procedure (DOC 4.4)
 - d. Risk treatment plan (DOC 4.1)
- 14. Section 5
 - a. Separate copy of the Information Security Policy
 - b. Management reviews
- 15. Section 6 (organizing information security)
 - a. Management commitment
 - b. Information security coordination
 - c. Authorization of facilities
 - d. Confidentiality agreements
 - e. Independent review of information security
 - f. External parties
 - g. Work instruction and schedule for authorities and key suppliers
- 16. Section 7 (asset management)
 - a. Asset inventory
 - b. Internet Acceptable Use policy
 - c. Rules for e-mail usage
 - d. Information security classification
 - e. Telecommunications requirements
 - f. Work instructions covering surf control, mail, mailbox sizes, voice mail, fax machines, photocopiers
 - g. Schedules for hardware assets, software log, information assets, intangible assets
- 17. Section 8 (human resources security)
 - a. Schedule of adjustments required to HR policies and procedures
 - b. Screening requirements procedure
 - c. Employee termination requirements and checklist
- 18. Section 9 (physical security)
 - a. Physical entry controls
 - b. Equipment security
 - c. Disposals of information equipment, devices and media
 - d. Off-site removals authorizations
 - e. Loading and unloading
 - f. Physical perimeter – security checklist

Complete BS7799/ISO17799 Documentation Toolkit

- g. Disposal log
 - h. Work instructions for fire doors, fire alarms, burglar alarms, fire suppression equipment, air conditioning, reception management and notebook configuration
19. Section 10 (Communications and operations management)
- a. Procedure covering the requirement to have documented procedures
 - b. Change control procedures
 - c. Separation of operational, test and development environments
 - d. Managing third parties
 - e. System planning and acceptance
 - f. Policy against malicious code
 - g. Anti-malware procedures
 - h. Backup
 - i. Network management
 - j. Media handling
 - k. Business information systems
 - l. E-commerce
 - m. Work instructions for anti-malware software, user name administration, privacy statements, website terms, change requests
 - n. Schedules for monitoring, administrator logging, off-site removals request log, change request log
20. Section 11 (access control)
- a. Access control policy
 - b. User access rights
 - c. User registration
 - d. User agreement (with addendums for mobile phone users, wireless notebook users)
 - e. Teleworkers – procedure
 - f. Teleworker user agreement
 - g. Teleworker checklist
 - h. Network access policy
 - i. Access control procedure
 - j. Secure log-on
 - k. System utilities
 - l. Mobile computing
 - m. Work instructions – replacement passwords, deletion request
21. Section 12 (Information systems acquisition)
- a. Control of cryptographic keys
 - b. Control of operational software
 - c. Vulnerability management
 - d. Schedule for cryptographic controls
22. Section 13 (incident management)
- a. Reporting information security events
 - b. Responding to information security incidents
 - c. Evidence collection
 - d. Event report and event report log
23. Section 14 (business continuity management)
- a. Business continuity planning
 - b. The Business Continuity Plan
 - c. Business continuity risk assessments
 - d. Testing, maintaining and re-assessing business continuity plans
24. Section 15 (compliance)
- a. Intellectual property rights compliance policy
 - b. IPR compliance procedure

Complete BS7799/ISO17799 Documentation Toolkit

- c. Safeguarding organizational records
- d. Data protection and privacy protection policy
- e. Compliance and compliance checking
- f. Systems auditing

BENEFITS OF THE *BS7799/ISO17799 DOCUMENTATION TOOLKIT*:

- Accelerates your BS7799/ISO17799 project
- Reduces your project (internal resource and external support) costs
- Cost-effectively deploys best practice
- Makes you your own expert
- Ensures that all the BS7799/ISO17799 control areas and controls are comprehensively and professionally addressed
- Avoids costly, credibility-destroying trial-and-error methods
- Accelerates organizational learning
- Crystallizes your approach to complex issues
- Catalyses how you deal with specific threats and controls
- Pre-written model policies and processes account for all the key issues
- Templated forms and documents save you time
- Integrates with the practical, detailed advice in "[*IT Governance: a Manager's Guide to Data Security and BS7799/ISO17799*](#)".

"IT Governance: a Manager's Guide to Data Security and BS7799/ISO17799"

"This book provides a comprehensive guide as to actions that should be taken." NIGEL TURNBULL, Chairman, Lasmco Plc, author of the Turnbull Report.

"The book underpins professional practice in InfoSec Management. Following the standard, risk management guidance is given for each InfoSec area, including the trade-offs that arise between covering a vulnerability and leaving it uncovered. For complete coverage of the standard, this book is unparalleled, and that's why we have chosen it as the basis for the Open University's new Information Security Management Course." Dr Jon G Hall, Lecturer in Information Security, Open University, UK.

"This book is essential reading for anyone involved in preparing for and maintaining BS7799 certification within their organisation. It is not only essential reading, but also a critical source when preparing and managing the ISMS. We used it extensively as a key reference during our BS7799 certification activities over the past two years. Without this source of practical advice the task would have been significantly harder." Bill Pepper Director of Security Risk Management CSC NR Royal Pavilion

"'IT Governance: a Manager's Guide to Data Security and BS7799/ISO17799' is a clear and authoritative guide to this important standard. It gives a through coverage of the requirements of the standard and practical guidance on what actions to take to achieve compliance with it." Roger Pawling, Countryside Council for Wales

"When faced with a security issue our IT adviser often refers to this book, referring to it as his 'information security management bible'." Justin Potter, Chairman, PDM Group.