IT Governance's Complete ISO27001/ISO27002 Documentation Toolkit

Why do I need the ISO27001/ISO27002 Documentation Toolkit?

- This toolkit contains ten years of ISO27001 (previously BS7799) implementation experience - so you get tested, pragmatic solutions.
- It is precisely tailored to the requirements of ISO27001/ISO27002 – it doesn't contain hundreds and hundreds of generic policies (ISO27001 only requires seven), but it does contain exactly the documents that you will need if you are serious about achieving certification – so your customisation time is minimised.
- It is comprehensive:
  - 120 different pre-written documents, totalling nearly 450 pages
  - See the detailed contents list below
- Our unique document support service enables you to get answers to documentation queries and conundrums within 24 hours – and at no extra cost to you.
- Our free updating service means that you will benefit from 12 months of updates and improvements to the toolkit, again at no extra cost.
- No software to install – just a comprehensive set of easy-to-customise Word documents that can easily be given your corporate look and feel.

"This Documentation Toolkit is a unique blend of an outstanding, practical and comprehensive suite of pre-written document templates and value-added services that will ***save you months of work*** and get your ISO27001/ISO27002 project off to a flying start." Alan Calder, author of *IT Governance: a Manager's Guide to Data Security and ISO27001/ISO27002.*

Detailed contents list for the ISO27001/ISO27002 Documentation Toolkit

1. Contents List and details of upgrades to recent versions
2. Graphical Visio representation of contents of documentation toolkit (excluding RA2 and vsRisk™ sub-folders), enabling you to see, at a glance, how the components fit together.
3. Introduction and user guidance for the ***ISO27001 Documentation Toolkit***
4. Blank templates:
   a. Policy, procedure, work instructions, meeting agenda, meeting minutes, schedule, checklist
5. Blank SLA template with detailed guidance on completion
6. ISMS Project Management Tools
   a. Documentation Implementation Manager, to control and manage all the micro-elements of the project
   b. Document & roles/responsibilities management tool
   c. Project team slide presentation 'What is an ISMS and why us?'
   d. PDCA cycle and documentation pyramid
   e. Entity-level security assessment tool
   f. High-level gap analysis and audit tool
7. 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 ISO27001 (also published as BS7799-2:2005 in the UK) and ISO27002
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. Designed to be customized and adapted for your organization and your legal jurisdiction.
i. Designed to be capable of integration with existing risk and quality management frameworks inside your organization

ISO27001/ISO27002 MODEL DOCUMENTS CONTAINED IN THE TOOLKIT

8. Risk Assessment Integration Documentation Folder, including integration user instructions and adapted versions of relevant templates for both RA2 and vsRisk™ Risk Assessment Tools.
9. Information Security Policy (DOC 5.1)
10. Statement of Applicability (contained in the ISMS Manual)
11. ISMS Manual (Information Security Manual)
12. Business continuity plan (section 14 of ISO27002:2005) (DOC 14.3)
13. Section 2 (of the Information Security Manual and 4.3 of ISO27001:2005)
    a. Document control procedure (DOC ISMS 1)
    b. Control of records procedure (DOC ISMS 2)
    c. Internal audit procedure (DOC MS-1)
    d. Corrective Action, Preventive Action Procedure (DOC MS-2)
    e. Internal Audit Report Lead Sheet (Rec MS-2A)
    f. Internal Audit Schedule (Rec MS-1A)
    g. Non-conformance report (Rec MS-3A)
    h. Non-conformance report log (Rec MS-4A)
14. Section 3
    a. Agendas for two management meetings, to initiate and to establish the ISMS
    b. Draft minutes of two management meetings, to initiate the project and establish the ISMS and approve the risk management framework
    c. Effectiveness Measurements Procedure (DOC 3.1)
15. Section 4 (base documents and tool-specific versions contained within the Section 4 Risk Assessment folder)
    a. Risk assessment tool selection (DOC 4.2)
    b. Risk management framework (DOC 4.3)
    c. Risk assessment procedure (DOC 4.4)
    d. Risk treatment plan (DOC 4.1)
16. Section 5
    a. Separate copy of the Information Security Policy (D0C 5.1)
    b. Management reviews (DOC 5.2)
17. Section 6 (organizing information security)
    a. Information Security Committee (DOC 6.1)
    b. Information security coordination (DOC 6.2)
    c. Authorization of facilities (DOC 6.4)
    d. Confidentiality agreements (DOC 6.5)

   e. Independent review of information security (DOC 6.7)
   f. External parties (DOC 6.8)
   g. Contact with authorities Work instruction (DOC 6.6)
   h. schedule for authorities and key suppliers (REC 6.6A)
18. Section 7 (asset management)
   a. Asset inventory (DOC 7.1)
   b. Internet Acceptable Use policy (DOC 7.2)
   c. Rules for e-mail usage (DOC 7.3)
   d. Information security classification (DOC 7.6)
   e. Telecommunications requirements (DOC 7.11)
   f. Work instructions covering surf control (DOC 7.4), mail/post (DOC 7.7), mailbox sizes (DOC 7.5), voice mail (DOC 7.8), fax machines (DOC 7.9), photocopiers (DOC 7.10)
   g. Schedules for hardware assets (REC 7.1A), software log (REC 7.1B), information assets (REC 7.1C), intangible assets (REC 7.1D)
19. Section 8 (human resources security)
   a. Schedule of adjustments required to HR policies and procedures
   b. Screening requirements procedure (DOC 8.1)
   c. Employee termination requirements (DOC 8.3) and checklist (REC 8.2a)
20. Section 9 (physical security)
   a. Physical entry controls (DOC 9.8)
   b. Equipment security DOC (9.10)
   c. Disposals of information equipment, devices and media (DOC 9.11)
   d. Off-site removals authorizations (DOC 9.12)
   e. Loading and unloading (DOC 9.9)
   f. Physical perimeter – security checklist (DOC 9.7)
   g. Disposal log (REC 9.1)
   h. Work instructions for fire doors (DOC 9.1), fire alarms (DOC 9.2), burglar alarms (DOC 9.3), fire suppression equipment (D0C 9.4), air conditioning (DOC 9.5), reception management (DOC 9.6) and notebook configuration (DOC 9.13)
21. Section 10 (Communications and operations management)
   a. Procedure covering the requirement to have documented procedures (DOC 10.1)
   b. Change control procedures (DOC 10.7)
   c. Separation of operational, test and development environments (DOC 10.8)
   d. Managing third parties (DOC 10.9)
   e. System planning and acceptance (DOC 10.10)
   f. Policy against malicious code (DOC 10.11)
   g. Controls against malicious code procedures (DOC 10.12)
   h. Backup (DOC 10.13)
   i. Network management (D0C 10.14)
   j. Media handling (DOC 10.15)
   k. Business information systems (DOC 10.16)
   l. E-commerce (D0C 10.17)
   m. Monitoring (DOC 10.18)
   n. Work instructions for anti-malware software (DOC 10.2), user name administration (DOC 10.3), privacy statements (DOC 10.4), Website terms (DOC 10.5), change requests (REC 10.3)
   o. Schedules for monitoring (DOC 10.20), administrator logging (DOC 10.21), off-site removals request log (DOC 10.1), change request log (REC 10.2), audit logging (DOC 10.19)
22. Section 11 (access control)
   a. Access control policy (DOC 11.1)
   b. User access rights (D0C 11.2)

   c. User registration (DOC 11.3)
   d. User Agreement (DOC 11.4) (with addendums for mobile phone users (DOC 11.6), wireless notebook users (DOC 11.5))
   e. Teleworkers – procedure (DOC 11.12)
   f. Teleworker user agreement (DOC 11.13)
   g. Teleworker checklist (REC 11.3)
   h. Network access policy (DOC 11.7)
   i. Access control procedure (DOC 11.8)
   j. Secure log-on (DOC 11.9)
   k. System utilities (DOC 11.10)
   l. Mobile computing (DOC 11.11)
   m. Work instructions – replacement passwords (REC 11.1), deletion request (REC 11.2)
23. Section 12 (Information systems acquisition)
   a. Control of cryptographic keys (DOC 12.2)
   b. Control of operational software (DOC 12.3)
   c. Vulnerability management (DOC 12.4)
   d. Schedule for cryptographic controls (DOC 12.1)
24. Section 13 (incident management)
   a. Reporting information security events (DOC 13.1)
   b. Responding to information security incidents (DOC 13.2)
   c. Evidence collection (DOC 13.4)
   d. Event report (REC 13.1A) and event report log (REC 13.5)
25. Section 14 (business continuity management)
   a. Business continuity planning (DOC 14.1)
   b. The Business Continuity Plan (DOC 14.3)
   c. Business continuity risk assessments (DOC 14.2)
   d. Testing, maintaining and re-assessing business continuity plans (DOC 14.4)
26. Section 15 (compliance)
   a. Intellectual property rights compliance policy (DOC 15.1)
   b. IPR compliance procedure (DOC 15.3)
   c. Retention of records (DOC 15.2)
   d. Data protection and privacy protection policy (D0C 15.6)
   e. Compliance and compliance checking (DOC 15.4)
   f. Systems auditing (DOC 15.5)

IT Governance's Complete ISO27001/ISO27002 Documentation Toolkit

Summary of your benefits from using this Documentation Toolkit

- Accelerates your ISO27001/ISO27002 compliance project;
- Provides clear guidance on the role of risk assessment;
- Reduces your total project costs (both internal and external);
- Cost-effectively deploys best practice;
- Makes you your own expert;
- Ensures that all ISO27001/ISO27002 control areas and controls are covered comprehensively and are professionally addressed;
- Avoids costly, credibility-destroying trial-and-error methods;
- Accelerates organizational learning;
- Crystallises your approach to complex issues;
- Catalyses how you deal with specific risks and controls;
- Pre-written model policies and procedure templates account for all the key issues in compliance with all aspects of the standards;
- Templated forms save you time and effort;
- Integrates perfectly with the best practice guidance in *IT Governance: a Manager's Guide to Data Security and ISO27001/ISO27002 (4th Edition).*

The No 4 ISMS Toolkit contains, in addition to the Documentation Toolkit,
IT Governance: a Manager's Guide to Data Security and ISO27001/ISO27002, 4th edition (ITG4)
A comprehensive online glossary

The No 5 ISMS Toolkit contains, in addition to the contents of the No 4 Toolkit,
Copies of both ISO 27001 and ISO 27002

The No 1 ISMS Toolkit contains, in addition to the contents of the No 5 Toolkit,
BS7799-3, the risk assessment standard

The No 3 ISMS Toolkit contains, in addition to the contents of the No 1 Toolkit,
vsRisk™, the definitive risk assessment tool

The No 2 ISMS Toolkit is the same as the No 3 Toolkit, except that it doesn't contain the three information security standards.

The choice between **UK/EU** and **US/RoW** editions of the toolkit reflects only the fact that the UK/EU versions have a copy of *ITG3*, whereas the US/RoW edition has a copy of the international version of ITG3, *International IT Governance: an Executive Guide to ISO 27001*.

The standalone, No 3 and No 4 Toolkits are all available with the documentation component either on CD-Rom or via download. All other components of all the kits are hard copies.

Toolkit	Doc. Toolkit	ISO 27001	ISO 17799	BS 7799 - 3	ITG4	vsRisk	UK/EU	US/RoW
No 1	√	√	√	√	√		√	√
No 2	√				√	√	√	√
No 3	√	√	√	√	√	√	√	√
No 4	√				√		√	√
No 5	√	√	√		√		√	√
Standalone	√						√	√