

DIN ISO/IEC 27001:2008-09 (E)

Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2005)

| Contents | Page |
|---|------|
| National foreword | 6 |
| National Annex NA (informative) Bibliography | 6 |
| 0 Introduction | 4 |
| 0.1 General | 4 |
| 0.2 Process approach | 4 |
| 0.3 Compatibility with other management systems | 5 |
| 1 Scope | 6 |
| 1.1 General | 6 |
| 1.2 Application | 6 |
| 2 Normative references | 6 |
| 3 Terms and definitions | 7 |
| 4 Information security management system | 8 |
| 4.1 General requirements | 8 |
| 4.2 Establishing and managing the ISMS | 9 |
| 4.2.1 Establish the ISMS | 9 |
| 4.2.2 Implement and operate the ISMS | 11 |
| 4.2.3 Monitor and review the ISMS | 11 |
| 4.2.4 Maintain and improve the ISMS | 12 |
| 4.3 Documentation requirements | 12 |
| 4.3.1 General | 12 |
| 4.3.2 Control of documents | 13 |
| 4.3.3 Control of records | 13 |
| 5 Management responsibility | 14 |
| 5.1 Management commitment | 14 |
| 5.2 Resource management | 14 |
| 5.2.1 Provision of resources | 14 |
| 5.2.2 Training, awareness and competence | 14 |
| 6 Internal ISMS audits | 15 |
| 7 Management review of the ISMS | 15 |
| 7.1 General | 15 |
| 7.2 Review input | 15 |
| 7.3 Review output | 16 |
| 8 ISMS improvement | 16 |
| 8.1 Continual improvement | 16 |
| 8.2 Corrective action | 16 |
| 8.3 Preventive action | 17 |
| Annex A (normative) Control objectives and controls | 18 |
| Annex B (informative) OECD principles and this International Standard | 35 |

| | |
|---|-----------|
| Annex C (informative) Correspondence between ISO 9001:2000, ISO 14001:2004 and this International Standard | 36 |
| Bibliography | 39 |