23 Thistledown, 12 Springside Road
Hillcrest
KwaZulu Natal
3650
South Africa

Specialists in ISO Management Systems
Planning, Implementation, Maintenance, Auditing & Training

ISO 27001:2013 Information Security Management Systems - Requirements (Summary) (Published 10-01-2013)

1. Scope
   "This International Standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation. This International Standard also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organisation. The requirements set out in this International Standard are generic and are intended to be applicable to all organisations, regardless of type, size or nature. Excluding any of the requirements specified in Clauses 4 to 10 is no acceptable when an organisation claims conformity to this International Standard."
2. Normative reference
3. Terms and definitions
   The terms and definitions given in ISO/IEC 27000 apply
4. Context of the organisation
   - 4.1 Understanding the organisation and it context
   - 4.2 Understanding the needs and expectations of interested parties
   - 4.3 Determining the scope of the Information Security Management System
   - 4.4 Information Security Management System
5. Leadership
   - 5.1 Leadership and commitment
   - 5.2 Policy
   - 5.3 Organisational roles, responsibilities and authorities
6. Planning
   - 6.1 Actions to address risks and opportunities
     - 6.1.1 General
     - 6.1.2 Information Security Risk assessment
     - 6.1.3 Information Security Risk Treatment
   - 6.2 Information Security Objectives and Planning to achieve them
7. Support
   - 7.1 Resources
   - 7.2 Competence
   - 7.3 Awareness
   - 7.4 Communication
   - 7.5 Documented information
     - 7.5.1 General
       "NOTE 1 The extent of documented information for an information security management system can differ from one organisation to another…"
     - 7.5.2 Creating and updating
     - 7.5.3 Control of documented information
8. Operation
   - 8.1 Operational planning and control
   - 8.2 Information Security Risk Assessment
   - 8.3 Information Security Risk Treatment
9. Performance evaluation
   - 9.1 Monitoring, measurement, analysis and evaluation
   - 9.2 Internal Audit
   - 9.3 Management review
10. Improvement
    - 10.1 Nonconformity and Corrective Action

10.2 Continual improvement

Reference:
ISO 27001:2013 Information security management system - requirements