

ISO/IEC 27000:2016-02 (E)

Information technology - Security techniques - Information security management systems - Overview and vocabulary

Contents		Page
Foreword	v
0	Introduction	1
0.1	Overview	1
0.2	ISMS family of standards	1
0.3	Purpose of this International Standard	2
1	Scope	2
2	Terms and definitions	2
3	Information security management systems	14
3.1	General	14
3.2	What is an ISMS?	14
3.2.1	Overview and principles	14
3.2.2	Information	15
3.2.3	Information security	15
3.2.4	Management	15
3.2.5	Management system	16
3.3	Process approach	16
3.4	Why an ISMS is important	16
3.5	Establishing, monitoring, maintaining and improving an ISMS	17
3.5.1	Overview	17
3.5.2	Identifying information security requirements	17
3.5.3	Assessing information security risks	18
3.5.4	Treating information security risks	18
3.5.5	Selecting and implementing controls	18
3.5.6	Monitor, maintain and improve the effectiveness of the ISMS	19
3.5.7	Continual improvement	19
3.6	ISMS critical success factors	20
3.7	Benefits of the ISMS family of standards	20
4	ISMS family of standards	21
4.1	General information	21
4.2	Standards describing an overview and terminology	22
4.3	Standards specifying requirements	22
4.4	Standards describing general guidelines	22
4.5	Standards describing sector-specific guidelines	25
4.5.7	ISO 27799	26
Annex A (informative)	Verbal forms for the expression of provisions	28
Annex B (informative)	Term and term ownership	29
Bibliography	33