

ISO/IEC 27102:2019-08 (E)

Information security management - Guidelines for cyber-insurance

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Structure of this document	2
5	Overview of cyber-insurance and cyber-insurance policy	2
5.1	Cyber-insurance	2
5.2	Cyber-insurance policy	3
6	Cyber-risk and insurance coverage	3
6.1	Risk management process and cyber-insurance	3
6.2	Cyber-incidents	4
6.2.1	General	4
6.2.2	Cyber-incident types	4
6.3	Business impact and insurable losses	4
6.3.1	Overview	4
6.3.2	Type of coverage	5
6.3.3	Liability	5
6.3.4	Incident response costs	5
6.3.5	Cyber-extortion costs	7
6.3.6	Business interruption	7
6.3.7	Legal and regulatory fines and penalties	7
6.3.8	Contractual penalties	7
6.3.9	Systems damage	8
6.4	Supplier risk	8
6.5	Silent or non-affirmative coverage in other insurance policies	8
6.6	Vendors and counsel for incident response	8
6.7	Cyber-insurance policy exclusions	8
6.8	Coverage amount limits	9
7	Risk assessment supporting cyber-insurance underwriting	9
7.1	Overview	9
7.2	Information collection	9
7.3	Cyber-risk assessment of the insured	10
7.3.1	General	10
7.3.2	Inherent cyber-risk assessment	10
7.3.3	Information security controls assessment	10
7.3.4	Review prior cyber-losses	11
8	Role of ISMS in support of cyber-insurance	11
8.1	Overview	11
8.2	ISMS as a source of information	12
8.2.1	ISMS	12
8.2.2	Planning	12
8.2.3	Support	13

8.2.4	Operation	13
8.2.5	Performance evaluation	14
8.2.6	Improvement	14
8.3	Sharing of information about risks and controls	14
8.4	Meeting cyber-insurance policy obligations	15
Annex A (informative) Examples of ISMS documents for sharing		16
Bibliography		17