

ISO/IEC 27036-4:2016-10 (E)

Information technology - Security techniques - Information security for supplier relationships - Part 4: Guidelines for security of cloud services

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	Key cloud concepts and security threats and risks	2
5.1	Characteristics of cloud computing	2
5.2	Cloud service threats and associated risks to the cloud service customer	3
5.3	Cloud service threats and associated risks for public cloud deployment model	4
5.4	Cloud service threats and associated risks for hybrid cloud deployment model	5
5.5	Cloud service threats and associated risks for private cloud deployment model	5
6	Information security controls in cloud service acquisition lifecycle	6
6.1	Agreement processes	6
6.1.1	Acquisition process	6
6.1.2	Supply process	7
6.2	Organizational project-enabling processes	8
6.3	Project processes	8
6.3.1	Project planning process	8
6.3.2	Project assessment and control process	8
6.3.3	Decision management process	8
6.3.4	Risk management process	8
6.3.5	Configuration management process	8
6.3.6	Information management process	9
6.3.7	Measurement process	9
6.4	Technical processes	9
6.4.1	Stakeholder requirements definition process	9
6.4.2	Requirements analysis process	9
6.4.3	Architectural design process	9
6.4.4	Implementation process	9
6.4.5	Integration process	10
6.4.6	Verification process	10
6.4.7	Transition process	10
6.4.8	Validation process	10
6.4.9	Operation process	10
6.4.10	Maintenance process	10
6.4.11	Disposal process	11
7	Information security controls in cloud service providers	11
7.1	Overview	11
7.1.1	Control sets related to cloud service deployment model	11
7.1.2	Setting information security controls at a cloud service provider	11
7.2	Public cloud deployment model	12
7.2.1	Infrastructure capabilities type	12

7.2.2	Platform capabilities type	13
7.2.3	Application capabilities type	13
7.3	Hybrid cloud deployment model	14
7.4	Private cloud deployment model	14
Annex A (informative) Information security standards for cloud providers		15
Bibliography		21