

ISO/IEC 27036-2:2022-06 (E)

Cybersecurity - Supplier relationships - Part 2: Requirements

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Abbreviated terms	1
5	Structure of this document	2
5.1	Clause 6	2
5.1.1	General	2
5.1.2	Organizational project-enabling processes	2
5.1.3	Technical management processes	2
5.2	Clause 7	3
5.3	Relationship between Clause 6 and Clause 7	3
5.4	Annexes	5
6	Information security in supplier relationship management	5
6.1	Agreement processes	5
6.1.1	Acquisition process	5
6.1.2	Supply process	7
6.2	Organizational project-enabling processes	8
6.2.1	Life cycle model management process	8
6.2.2	Infrastructure management process	8
6.2.3	Project portfolio management process	9
6.2.4	Human resource management process	9
6.2.5	Quality management process	10
6.2.6	Knowledge management process	10
6.3	Technical management processes	11
6.3.1	Project planning process	11
6.3.2	Project assessment and control process	11
6.3.3	Decision management process	11
6.3.4	Risk management process	11
6.3.5	Configuration management process	13
6.3.6	Information management process	13
6.3.7	Measurement process	13
6.3.8	Quality assurance process	14
6.4	Technical processes	14
6.4.1	Business or mission analysis process	14
6.4.2	Architecture definition process	14
7	Information security in a supplier relationship instance	15
7.1	Supplier relationship planning process	15
7.1.1	Objective	15
7.1.2	Inputs	15
7.1.3	Activities	15
7.1.4	Outputs	16
7.2	Supplier selection process	17
7.2.1	Objectives	17
7.2.2	Inputs	17
7.2.3	Activities	17

7.2.4	Outputs	21
7.3	Supplier relationship agreement process.....	21
7.3.1	Objective.....	21
7.3.2	Inputs.....	22
7.3.3	Activities.....	22
7.3.4	Outputs	24
7.4	Supplier relationship management process.....	25
7.4.1	Objectives	25
7.4.2	Inputs.....	26
7.4.3	Activities.....	26
7.4.4	Outputs	27
7.5	Supplier relationship termination process.....	28
7.5.1	Objectives	28
7.5.2	Inputs.....	28
7.5.3	Activities.....	28
7.5.4	Outputs	29
Annex A (informative) Correspondence between ISO/IEC/IEEE 15288 and this document.....		30
Annex B (informative) Correspondence between ISO/IEC 27002 controls and this document.....		32
Annex C (informative) Objectives from Clauses 6 and 7.....		34
Bibliography.....		38