ISO/IEC 27036-3:2013-11 (E)

Information technology - Security techniques - Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 1

4 Structure of this standard 2

5 Key concepts 2
5.1 Business case for ICT supply chain security 2
5.2 ICT supply chain risks and associated threats 3
5.3 Acquirer and supplier relationship types 3
5.4 Organizational capability 4
5.5 System lifecycle processes 4
5.6 ISMS processes in relation to system lifecycle processes 5
5.7 ISMS information security controls in relation to ICT supply chain security 5
5.8 Essential ICT supply chain security practices 5

6 ICT supply chain security in Lifecycle Processes 7
6.1 Agreement Processes 7
6.2 Organizational Project-Enabling Processes 10
6.3 Project Processes 13
6.4 Technical Processes 15

Annex A (informative) Summary of Supply and Acquisition Processes from ISO/IEC 15288 and ISO/IEC 12207 24

Annex B (informative) Clause 6 mapping to ISO/IEC 27002 35

Bibliography 37