ISO/IEC 27036-3:2023-06 (E)

Cybersecurity - Supplier relationships - Part 3: Guidelines for hardware, software, and services supply chain security

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Structure **2**

5 Key concepts **2**
5.1 Business case for hardware, software, and services supply chain security 2
5.2 Hardware, software, and services supply chain risks and associated threats 3
5.3 Acquirer and supplier relationship types 3
5.4 Organizational capability 4
5.5 System life cycle processes 4
5.6 ISMS processes in relation to system life cycle processes 5
5.7 ISMS controls in relation to hardware, software, and services supply chain security 6
5.8 Essential hardware, software, and services supply chain security practices 6

6 Hardware, software, and services supply chain security in life cycle processes **7**
6.1 Agreement processes 7
6.1.1 Acquisition process 7
6.1.2 Supply process 9
6.2 Organizational project-enabling processes 11
6.2.1 Life cycle model management process 11
6.2.2 Infrastructure management process 11
6.2.3 Project portfolio management process 12
6.2.4 Human resource management process 12
6.2.5 Quality management process 13
6.2.6 Knowledge management process 13
6.3 Technical management processes 13
6.3.1 Project planning process 13
6.3.2 Project assessment and control process 14
6.3.3 Decision management process 14
6.3.4 Risk management process 14
6.3.5 Configuration management process 15
6.3.6 Information management process 16
6.3.7 Measurement process 16
6.3.8 Quality assurance process 16
6.4 Technical processes 16
6.4.1 Business or mission analysis process 16
6.4.2 Stakeholder needs and requirements definition process 16
6.4.3 System requirements definition process 17
6.4.4 System architecture definition process 18
6.4.5 Design definition process 19
6.4.6 System analysis process 19
6.4.7 Implementation process 19
6.4.8 Integration process 20
6.4.9 Verification process 20
6.4.10 Transition process 21

6.4.11 Validation process 22
6.4.12 Operation process 23
6.4.13 Maintenance process 23
6.4.14 Disposal process 24

Annex A (informative) **Correspondence between the controls in ISO/IEC 27002 and this document** **26**

Annex B (informative) **Essential elements of a software bill of materials** **29**

Bibliography **34**