

# 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

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
Introduction .....		v
<b>1</b>	<b>Scope .....</b>	<b>1</b>
<b>2</b>	<b>Normative references .....</b>	<b>1</b>
<b>3</b>	<b>Terms and definitions .....</b>	<b>1</b>
<b>4</b>	<b>Structure of this standard .....</b>	<b>2</b>
<b>5</b>	<b>Key concepts .....</b>	<b>2</b>
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
<b>6</b>	<b>ICT supply chain security in Lifecycle Processes .....</b>	<b>7</b>
6.1	Agreement Processes .....	7
6.2	Organizational Project-Enabling Processes .....	10
6.3	Project Processes .....	13
6.4	Technical Processes .....	15
<b>Annex A (informative)</b>	<b>Summary of Supply and Acquisition Processes from ISO/IEC 15288 and ISO/IEC 12207 .....</b>	<b>24</b>
<b>Annex B (informative)</b>	<b>Clause 6 mapping to ISO/IEC 27002 .....</b>	<b>35</b>
<b>Bibliography .....</b>		<b>37</b>