



BSI Standards Publication

## Cybersecurity — Supplier relationships

---

Part 2: Requirements

## National foreword

This British Standard is the UK implementation of ISO/IEC 27036-2:2022. It supersedes BS ISO/IEC 27036-2:2014, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33, Information security, cybersecurity and privacy protection.

A list of organizations represented on this committee can be obtained on request to its committee manager.

### Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2022  
Published by BSI Standards Limited 2022

ISBN 978 0 539 16030 7

ICS 35.030

**Compliance with a British Standard cannot confer immunity from legal obligations.**

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 August 2022.

### Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

# INTERNATIONAL STANDARD

**ISO/IEC**  
**27036-2**

Second edition  
2022-06

---

---

## **Cybersecurity — Supplier relationships —**

### **Part 2: Requirements**

*Partie 2: Exigences*



Reference number  
ISO/IEC 27036-2:2022(E)



## **COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2022

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
CP 401 • Ch. de Blandonnet 8  
CH-1214 Vernier, Geneva  
Phone: +41 22 749 01 11  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

<b>Foreword</b>	<b>v</b>
<b>Introduction</b>	<b>vi</b>
<b>1 Scope</b>	<b>1</b>
<b>2 Normative references</b>	<b>1</b>
<b>3 Terms and definitions</b>	<b>1</b>
<b>4 Abbreviated terms</b>	<b>1</b>
<b>5 Structure of this document</b>	<b>2</b>
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 <a href="#">Clause 6</a> and <a href="#">Clause 7</a>	3
5.4 Annexes	5
<b>6 Information security in supplier relationship management</b>	<b>5</b>
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
<b>7 Information security in a supplier relationship instance</b>	<b>15</b>
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
<b>Annex A (informative) Correspondence between ISO/IEC/IEEE 15288 and this document .....</b>		<b>30</b>
<b>Annex B (informative) Correspondence between ISO/IEC 27002 controls and this document .....</b>		<b>32</b>
<b>Annex C (informative) Objectives from <a href="#">Clauses 6</a> and <a href="#">7</a> .....</b>		<b>34</b>
<b>Bibliography .....</b>		<b>38</b>