



DPC: 25/30497166 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 02 December 2025

Origin: International

Latest date for receipt of comments: 25 January 2026

Project No. 2024/02034

Responsible committee: IST/33/4 Security Controls and Services

Interested committees:

Title: Draft BS ISO/IEC 27045 Information security, cybersecurity and privacy protection — Big data security and privacy — Guidelines for managing big data risks.

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of the content of this standard:

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 25 January 2026

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

E-mail: admin.start@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



DRAFT International Standard

ISO/IEC DIS 27045

Information security, cybersecurity and privacy protection — Big data security and privacy — Guidelines for managing big data risks

ICS: 35.240.01; 35.030

ISO/IEC JTC 1/SC 27

Secretariat: **DIN**

Voting begins on:
2025-12-02

Voting terminates on:
2026-02-24

This document is circulated as received from the committee secretariat.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Reference number
ISO/IEC DIS 27045:2025(en)

Full document details: 25/30497166 DC

© ISO/IEC 2025  **Documents**
Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2025

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
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms, definitions and abbreviated terms	1
3.1 Terms and definitions	1
3.2 Abbreviated terms	3
4 Overview	3
5 Big data	4
5.1 General	4
5.2 Big data characteristics	4
6 Security and privacy threats and controls to big data	5
6.1 Volume-related threats and controls	5
6.1.1 Security threats	5
6.1.2 Security and privacy controls	6
6.2 Velocity-related threats and controls	6
6.2.1 Security threats	6
6.2.2 Security and privacy controls	6
6.3 Variety-related threats and controls	6
6.3.1 Security threats	6
6.3.2 Security and privacy controls	7
6.4 Variability-related threats and controls	7
6.4.1 Security threats	7
6.4.2 Security and privacy controls	7
6.5 Volatility-related threats and controls	8
6.5.1 Security threats	8
6.5.2 Security and privacy controls	8
6.6 Veracity-related threats and controls	8
6.6.1 Security threats	8
6.6.2 Security and privacy controls	8
6.7 Value-related threats and controls	8
6.7.1 Security threats	8
6.7.2 Security and privacy controls	9
6.8 Validity-related threats and controls	9
6.8.1 Security threats	9
6.8.2 Security and privacy controls	9
6.9 Potential threats and controls related to AI and LLMs	9
6.9.1 Security threats	9
6.9.2 Security and privacy controls	10
7 Big data risk management process	10
7.1 Establishing risk management framework	10
7.2 Risk identification	10
7.3 Risk analysis and evaluation	11
7.4 Risk treatment	11
7.5 Risk monitoring and review	11
Annex A (informative) Mapping between big data Vs and security and privacy controls	12
Annex B (informative) Use cases	15
Bibliography	16

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC JTC1, *Information Technology*, Subcommittee SC 27, Information security, cybersecurity and privacy protection.

Introduction

Big data technologies are used extensively across diverse industries such as retail, finance, healthcare, insurance and energy distribution. It is widely accepted that business development today relies on big data to a great extent. Security and privacy of big data can involve different strategies to augment traditional systems' controls for security and privacy.

Big data introduces unique security and privacy challenges that are affected by the additional risks associated with big data characteristics. These characteristics include high:

- volume,
- velocity,
- variety,
- variability,
- volatility,
- veracity,
- value and,
- validity.

These big data characteristics introduce additional risks to the security and privacy of big data for which traditional security safeguards are ineffective without additional controls being implemented.

The guidance in this document can help organizations achieve and scale their security and privacy objectives in a big data environment. This document also provides guidance for organizations to build their big data security capabilities.

