DRAFT International Standard

ISO/IEC DIS 27045.2

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:
2026-06-11

Voting terminates on:
2026-08-06

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.

This document has not been edited by the ISO Central Secretariat.

Reference number
ISO/IEC DIS 27045.2:2026(en)

© ISO/IEC 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

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 ... 4

4 Overview ... **4**

5 Introduction to big data ... **4**
5.1 General ... 4
5.2 Big data characteristics ... 5

6 Security and privacy threats and controls to big data ... **6**
6.1 Volume-related threats and controls ... 6
6.1.1 Security and privacy threats ... 6
6.1.2 Security and privacy controls ... 6
6.2 Velocity-related threats and controls ... 6
6.2.1 Security and privacy threats ... 6
6.2.2 Security and privacy controls ... 7
6.3 Variety-related threats and controls ... 7
6.3.1 Security and privacy threats ... 7
6.3.2 Security and privacy controls ... 7
6.4 Variability-related threats and controls ... 8
6.4.1 Security and privacy threats ... 8
6.4.2 Security and privacy controls ... 8
6.5 Volatility-related threats and controls ... 9
6.5.1 Security and privacy threats ... 9
6.5.2 Security and privacy controls ... 9
6.6 Veracity-related threats and controls ... 9
6.6.1 Security and privacy threats ... 9
6.6.2 Security and privacy controls ... 9
6.7 Value-related threats and controls ... 10
6.7.1 Security and privacy threats ... 10
6.7.2 Security and privacy controls ... 10
6.8 Validity-related threats and controls ... 10
6.8.1 Security and privacy threats ... 10
6.8.2 Security and privacy controls ... 11
6.9 Potential threats and controls related to AI and LLMs ... 11
6.9.1 Security and privacy threats ... 11
6.9.2 Security and privacy controls ... 11

7 Big data risk management process ... **12**
7.1 Establishing risk management framework ... 12
7.2 Risk identification ... 12
7.3 Risk analysis and evaluation ... 12
7.4 Risk treatment ... 12
7.5 Risk monitoring and review ... 13

Annex A (informative) **Mapping between big data characteristics and security and privacy controls** ... **14**

Annex B (informative) **Use cases** ... **19**

Bibliography ... **26**

© ISO/IEC 2026 – All rights reserved

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.

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 document 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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

For an explanation of 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 www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

© ISO/IEC 2026 – All rights reserved

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,

— 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.

© ISO/IEC 2026 – All rights reserved

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

1 Scope

This document provides guidelines on how to manage the risks and navigate the threats that can arise during the big data life cycle from the various big data characteristics that are unique to big data: volume, velocity, variety, variability, volatility, veracity, validity and value, including when using big data for the design and implementation of artificial intelligence (AI) systems.

This document can help organizations build or enhance their big data security and privacy capabilities, including when using big data in the development and use of AI systems. This document is applicable to all organizations that develop or use big data systems, regardless of their type, size or purpose.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 22989:2022, *Information technology — Artificial intelligence — Artificial intelligence concepts and terminology*

ISO/IEC 27005:2022, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27005, ISO/IEC 22989 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1.1
artificial intelligence system
AI system
engineered system that generates outputs such as content, forecasts, recommendations or decisions for a given set of human-defined objectives

[SOURCE: ISO/IEC 22989:2022, 3.1.4, modified — notes to entry have been removed.]

3.1.2
asset
anything that has value to an individual, an organization or a government

[SOURCE: ISO/IEC 27035-3:2020, 3.1]

© ISO/IEC 2026 – All rights reserved

3.1.3
availability
property of being accessible and useable upon demand by an authorized entity

[SOURCE: ISO/IEC 27000:—[1)], 3.4]

3.1.4
big data
extensive datasets primarily in the characteristics of volume, variety, velocity or variability that require a scalable architecture for efficient storage, manipulation, and analysis

[SOURCE: ISO/IEC 20546:2019, 3.1.2, modified — note 1 to entry has been removed.]

3.1.5
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[SOURCE: ISO/IEC 27000:—, 3.2]

3.1.6
data classification
process of analyzing structured or unstructured data and organizing it into categories based on its level of sensitivity and the impact should that data be disclosed, altered or destroyed without authorization

3.1.7
data life cycle
stages in the process of data usage from idea conception to its discontinuation

[SOURCE: ISO/IEC 5259-1:2024, 3.1]

3.1.8
integrity
property of accuracy and completeness

[SOURCE: ISO/IEC 27000:—, 3.3]

3.1.9
large language model
LLM
machine learning model that encodes the functioning of natural language with a large number of parameters and facilitates a variety of natural language processing tasks

3.1.10
privacy policy
overall intention and direction, rules and commitment, as formally expressed by the personally identifiable information (PII) controller related to the processing of PII in a particular setting

[SOURCE: ISO/IEC 29100:2024, 3.14]

3.1.11
risk
effect of uncertainty on objectives

[SOURCE: ISO/IEC 31000, 3.1, modified — notes to entry have been removed.]

3.1.12
security capability
characterization of the ability of an organization to implement security measures

1) Under preparation. Stage at the time of publication: ISO/FDIS 27000:2026.

© ISO/IEC 2026 – All rights reserved

3.1.13
threat
potential cause of an information security incident that can result in damage to a system or harm to an organization

[SOURCE: ISO/IEC 27005:2022, 3.1.9]

3.1.14
validity
relevance, quality, consistency, preciseness, and correctness of *big data* (3.1.4) according to its intended use

3.1.15
value
insights derived from big data discovery and pattern recognition that lead to more effective performance

3.1.16
variability
changes in transmission rate, format or structure, semantics, or quality of datasets

[SOURCE: ISO/IEC 20546:2019, 3.1.13]

3.1.17
variety
range of formats, logical models, timescales, semantics and sources of a dataset

Note 1 to entry: Data variety refers to irregular or heterogeneous data structures, their navigation, query, and data typing

[SOURCE: ISO/IEC 20546:2019, 3.1.14, modified, aspect of range of sources has been also included]

3.1.18
velocity
rate of flow at which data is created, transmitted, stored, analysed or visualised

[SOURCE: ISO/IEC 20546:2019, 3.1.15]

3.1.19
veracity
completeness and/or accuracy of data

Note 1 to entry: Data veracity refers to descriptive data and self-inquiry about objects to support real-time decision-making

[SOURCE: ISO/IEC 20546:2019, 3.1.16]

3.1.20
volatility
characteristic of data pertaining to the rate of change of these data over time

[SOURCE: ISO/IEC 20546:2019, 3.1.17]

3.1.21
volume
extent of the amount of data (3.1.5) relevant to impacting computation and storage resources and their management during data processing

Note 1 to entry: Data volume becomes important in dealing with large datasets

[SOURCE: ISO/IEC 20546:2019, 3.1.18, note to entry has been modified]

© ISO/IEC 2026 – All rights reserved

3.1.22
vulnerability
weakness of an asset or control that can be exploited so that an event with a negative consequence occurs

[SOURCE: ISO/IEC 27005:2022, 3.1.10]

3.2 Abbreviated terms

DPO	data protection officer
IAM	identity and access management
LLM	large language model
MPC	multi-party computation
PII	personally identifiable information

4 Overview

The key characteristics of big data such as volume, velocity, variety, variability, volatility, veracity and value introduce additional security risks and threats, especially with the rise of new services such as on-demand distributed computing power and storage from public cloud providers. Hence, big data security becomes an essential component of any big data system.

This document helps to identify and address security threats to big data throughout the big data life cycle, and provides guidelines for organizations to develop security measures for building their big data security and privacy capabilities. The security measures defined in this document can help to mitigate the risks arising from the characteristics of big data.

5 Introduction to big data

5.1 General

In the big data context, traditional security threats still exist, such as the advanced persistent threat (APT), distributed denial of service (DDoS) and data mining issues. The big data characteristics (see 5.2) introduce additional risks and threats on the security aspect of big data.

Furthermore, the traditional security techniques currently in use, for example, firewalls and other perimeter security tools, are not effective in a big data infrastructure. Some of the most notable big data security issues are as follows: fake data generation, multi-cloud computing vulnerabilities and data cleansing problems. Access control mechanisms need more granular privilege management. Distributed storing and processing of big data using different systems and devices would likely introduce additional security risks. For example, identifying potential attacks requires more analysis and more time to detect an event when managing big data.

In the context of big data, AI and LLMs introduce unique characteristics that can significantly impact security and privacy, as follows.

— Automated data generation: AI and LLMs can generate vast amounts of data autonomously, which can be difficult to trace or attribute to a specific source.

— Data complexity: The data processed by AI and LLMs can be highly complex, involving natural language, images, or other multimedia content, which requires sophisticated analysis techniques.

— Dynamic data evolution: As AI models learn and adapt, the data they generate or manipulate can evolve rapidly, posing challenges for traditional data management and security practices.

© ISO/IEC 2026 – All rights reserved