ISO/IEC 27046 — Information technology — **Big data security and privacy — Implementation guidelines** *[DRAFT]*

Abstract

"[ISO/IEC 27046] aims to analyze key challenges and risks of big data security and privacy, and propose guidelines for implementation of big data security and privacy in aspects of big data resources, and organizing, distributing, computing and destroying big data."

[Source: ISO/IEC JTC 1/SC 27 Committee Doc 11 May 2025]

Introduction

This standard was intended to help organisations implement the processes described in ISO/IEC 27045 in order to ensure the security and privacy of big data.

Scope and purpose

The standard may "address the key challenges and risks of big data security and privacy", providing guidance on how to:

- [Identify and] grade [evaluate?] big data security and privacy risks;
- Deploy [implement, use and manage] and maintain security and privacy controls [and other risk treatments?];
- Validate and verify big data security and privacy arrangements [to gain assurance].

The audiences include:

- "software and hardware providers to securely construct a big data framework";
- "application operators [service providers??] to securely maintain a big data framework";
- "data providers and consumers to securely realize big data functions [??];
- "industry to improve robustness and efficiency at the ecosystem level [??] to improve compatibility and inter-operation, to diversify choices of security products and to reduce redundant cost on security". [*from the 4th Working Draft*].

ISO/IEC 20547-4 *"Information technology - Big data reference architecture - Part 4: Security and privacy"* is cited as a normative (essential) reference.

Content of the standard

The standard may guide big data security and privacy planners, managers, implementers, operators and auditors, through a lifecycle sequence of big data:

ISO/IEC 27036
ISO/IEC 27037
ISO/IEC 27038
ISO/IEC 27039
ISO/IEC 27040
ISO/IEC 27041
ISO/IEC 27042
ISO/IEC 27043
ISO/IEC 27045
ISO/IEC 27046
ISO/IEC 27050
ISO/IEC 27070
ISO/IEC 27071
ISO/IEC 27090
ISO/IEC 27091
ISO/IEC 27099
ISO/IEC TS 27100
ISO/IEC 27102
ISO/IEC TR 27103
ISO/IEC TR 27109
ISO/IEC TS 27110
ISO/IEC TS 27115
ISO/IEC 27116
ISO/IEC 27400
ISO/IEC 27402
ISO/IEC 27403
ISO/IEC 27404
ISO/IEC TR 27550
ISO/IEC 27551
ISO/IEC 27553
ISO/IEC 27554
ISO/IEC 27555
ISO/IEC 27556
ISO/IEC 27557
ISO/IEC 27559
ISO/IEC TS 27560

- Collection - data are amassed from internal/corporate and external systems;
- Transmission - data pass between networks;
- Storage - stored in massive database systems, perhaps in the cloud;
- Processing - manipulating and analysing big data to gain useful insight;
- Exchange - information passes between organisations; and
- Destruction - securely and permanently destroying big data.

The applicable information security and privacy controls vary across the lifecycle, and are described succinctly in the standard through a set of action-oriented statements (*e.g.* in the big data transmission stage, one control is to "check the integrity of the transmitted data", with no further guidance about why that may be important nor how to do it). In effect, the standard is a generic checklist of suggested/potential controls to consider, adapt and adopt.

Status of the standard

The standard development project commenced in 2019 and reached **C**ommittee **D**raft stage before being halted due to the rebooting of the ISO/IEC 27045 project in 2023, returning to the **P**reliminary **W**ork **I**tem stage.

It is unlikely to surface before ISO/IEC 27045 is published in 2027 - so maybe 2028?

Personal comments

The definition of 'big data' in the draft standard did not (in my personal, rather jaundiced and cynical opinion) reflect its widespread use in the IT industry at present, mostly because of the vagueness of 'extensive' which is essentially synonymous with, and adds little clarity to, plain 'big'.

I find Wikipedia more helpful *e.g.*:

> *"Current usage of the term big data tends to refer to the use of predictive analytics, user behavior analytics, or certain other advanced data analytics methods that extract value from data, and seldom to a particular size of data set. "There is little doubt that the quantities of data now available are indeed large, but that's not the most relevant characteristic of this new data ecosystem." Analysis of data sets can find new correlations to "spot business trends, prevent diseases, combat crime and so on." Scientists, business executives, practitioners of medicine, advertising and governments alike regularly meet difficulties with large data-sets in areas including Internet searches, fintech, urban informatics, and business informatics. Scientists encounter limitations in e-Science work, including meteorology, genomics, connectomics, complex physics simulations, biology and environmental research."*

For me, one of the defining characteristics of big data is that typical (mostly relational) database management systems struggle or are unable to cope with the complexity and dynamics/volatility of truly massive data sets. Beyond the limits of their scalability, conventional architectures experience constraints and failures, no matter how much raw CPU power is thrown at the problems. That implies the need for fundamentally different approaches and I rather suspect entails novel information risks and hence security/privacy controls. However, it remains to be seen what this standard will actually address in practice: this is cutting-edge stuff.

I'm not sure how this standard will differ from and add value to the existing standard ISO/IEC 20547-4:2020.

The draft standard is not *explicitly* risk-driven: as shown above with a big data transmission control example, it simply recommends a bunch of security and privacy controls without clarifying the "key challenges and [information] risks" they are intended to mitigate - hence users of the standard may not appreciate their relative importance and relevance to the business, or to relevant compliance obligations and conformity requirements.

< Previous standard ^ Up a level ^ Next standard >

ISO/IEC 27561
ISO/IEC 27562
ISO/IEC TR 27563
ISO/IEC 27564
ISO/IEC 27565
ISO/IEC 27566
ISO/IEC 27568
ISO/IEC 27569
ISO/IEC TS 27570
ISO/IEC 27573
ISO/IEC 27701
ISO/IEC 27706
ISO 27799