ISO/IEC 27045 — Information technology — **Big data security and privacy — Guidelines for managing big data risks** *[DRAFT]*

Abstract

"[ISO/IEC 27045] provides guidance on how to 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 and value, including when using big data for the design and implementation of AI systems.

[ISO/IEC 27045] 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."

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

Introduction

'Big data' systems present numerous information security, privacy and technological challenges due to the system complexity, sheer quantity and volatility of the data.

Scope & purpose

The standard is intended to help organisations build or enhance their information security and privacy capabilities relating to big data systems, perhaps as part of AI systems design and implementation.

Content

The standard will outline potential threats plus security and privacy controls relating to the seven **v** characteristics of big data, namely **v**olume, **v**elocity, **v**ariety, **v**ariability, **v**olatility, **v**eracity and **v**alue.

Status

This standard was initially proposed in 2017.

Having run off-the-rails in 2021, the drafting project re-started in 2024.

Publication is now planned for 2027. It is at **C**ommittee **D**raft stage.

Personal comments

The definition of 'big data' quoted from ISO/IEC 20456:2019 does not (in my personal, rather jaundiced/cynical opinion) reflect its widespread use in the IT industry at present. "*Extensive datasets primarily in the characteristics of volume, variety, velocity, and/or variability that require a scalable architecture for efficient*

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

storage, manipulation, and analysis".

I prefer Wikipedia's description:

> *"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."*

It seems to me a defining characteristic is that big data is (are!) ***so*** big that conventional database management systems are unable to cope with the complexity and dynamics/volatility, struggling to maintain integrity given so many coincident changes. Beyond the limits of their scalability, conventional architectures start to experience constraints and failures (including security control and privacy issues), no matter how much raw CPU power, network bandwidth and storage capacity is thrown at the challenge. That implies the need for *fundamentally different approaches* with novel information risks most likely requiring novel controls. It remains to be seen what this standard will actually recommend: this is cutting-edge stuff.

Hopefully this standard will refer to others for the low-level and relatively conventional data security and privacy controls that apply to small and medium data, focusing instead on the high-level and novel aspects and processes that are unique to big data *e.g.*:

- Strategic management of big data sets, big data systems *etc.*, including governance arrangements to monitor and control the management and operational activities as a whole (*e.g.* overall programme as well as individual project management) and the business/strategy aspects and requirements (*e.g.* enormous financial investment in huge systems implies enormous expected returns);
- Architecture and design of big data systems - specifically the data security and privacy aspects including information risk assessment, compliance, ethics, data aggregation, inference, interconnectivity (both within and without the organisation), access controls, metadata management and security, resilience *etc.*;
- Operation and use of big data systems *e.g.* how to classify and segregate data and functions, how to determine/define and assign access rights/permissions, what privacy and security roles and responsibilities might be appropriate;
- Maintenance and support of big data systems, including their security and privacy aspects;
- Capacity and performance management including the dynamics and challenges arising;
- Incident management, change management and so on (adapting conventional processes for the big data environment).

Potentially, the standard *could* get into advanced/novel data/system security controls and privacy approaches involving artificial intelligence, instrumentation, anomaly and fraud detection, automated responses *etc.* ... but it looks as if the standard's initial release will be more modest.

< 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