
**Information technology — Big data
reference architecture —**

**Part 4:
Security and privacy**

*Technologies de l'information — Architecture de référence des
mégadonnées —*

Partie 4: Sécurité et confidentialité

This document is a preview generated by EBS



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2020

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	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	1
5 Overview	2
5.1 Big data security and privacy concerns	2
5.2 Security and privacy objectives	4
6 Security and privacy aspects of BDRA user view	6
6.1 Governance activities	6
6.1.1 Purpose	6
6.1.2 Prepare for and plan BD-S&P governance effort	7
6.1.3 Monitor, assess and control BD-S&P governance activities	7
6.1.4 Establish BD-S&P governance objectives	7
6.1.5 Direct BD-S&P	8
6.1.6 Monitor and assess compliance with BD-S&P governance directives and guidance	9
6.1.7 Review implementation of BD-S&P governance directives and guidance and prepare for change	9
6.2 Management activities	10
6.2.1 Purpose	10
6.2.2 Prepare for and plan BD-S&P management effort	10
6.2.3 Monitor, assess and control the architecture management activities	11
6.2.4 Develop BD-S&P management approach	11
6.2.5 Perform management of BD-S&P	12
6.2.6 Monitor BD-S&P effectiveness	12
6.2.7 Update the BD-S&P management plan	13
6.3 Operation activities	14
6.3.1 BD-S&P solution design activities	14
6.3.2 BD-S&P solution evaluation activities	19
6.3.3 BD-S&P solution enablement activities	23
6.4 Security and privacy aspects of big data roles	26
7 Guidance on security and privacy operations for big data	29
7.1 General	29
7.2 Guidance at organization level	30
7.2.1 General	30
7.2.2 Standard guidance on requirements	31
7.2.3 Standard guidance on risk management	32
7.2.4 Standard guidance on controls	32
7.2.5 Standard guidance on lifecycle operations	32
7.3 Guidance at ecosystem level	32
7.3.1 General	32
7.3.2 Guidance on data processing chain	33
7.3.3 Guidance on risk management	34
7.3.4 Guidance on lifecycle operations	35
8 Security and privacy functional components	37
8.1 Overview	37
8.2 Functional components for both security and privacy	37
8.3 Functional components for privacy	38
8.4 Multi-layer functions for security and privacy	39

Annex A (informative) Examples of security and privacy threat classification	41
Annex B (informative) Examples of security and privacy control classification	42
Annex C (informative) Examples of ecosystem and resulting coordination of security and privacy operations	45
Annex D (informative) Examples of security and privacy controls per BDRA roles	52
Bibliography	58

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO 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 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 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.

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.

A list of all parts in the ISO/IEC 20547 series can be found on the ISO website.

Introduction

Big data refers to the massive amount of digital information collected in various forms from different sources of digital and physical environments. This data is not only generated by traditional means of information exchange, but also from sensors embedded in physical environments, such as city surroundings, transportation vehicles, critical infrastructures, etc. The collection and processing of big data provides additional challenges not inherent in the traditional digital information exchange setting.

This document was developed in response to the worldwide demand for a common baseline of security and privacy aspects for big data architectures to facilitate interoperability in big data systems without compromising privacy, confidentiality, or integrity.

The big data paradigm blurs the security boundaries between data collection, storage and access — areas traditionally addressed independently — that now needs to be confronted holistically with a comprehensive security and privacy foundation, tightly coupled to all architecture components.

Effective standardization of security and privacy is paramount to the development of mutual trust and cooperation amongst big data stakeholders.

Information technology — Big data reference architecture —

Part 4: Security and privacy

1 Scope

This document specifies the security and privacy aspects applicable to the big data reference architecture (BDRA) including the big data roles, activities and functional components and also provides guidance on security and privacy operations for big data.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes the 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 20546, *Information technology — Big data — Overview and vocabulary*

ISO/IEC 20547-3, *Information technology — Big data reference architecture — Part 3: Reference architecture*

ISO/IEC/IEEE 15288, *Systems and software engineering — System life cycle processes*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 20546 apply.

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

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>

4 Symbols and abbreviated terms

APT	advanced persistent threat
BDRA	big data reference architecture
BD-S&P	big data security and privacy
DDoS	distributed denial of service
LINDDUN	linkability, identifiability, non-repudiation, detectability, disclosure of information, unawareness, non-compliance
PII	personally identifiable information
STRIDE	spoofing of user identity, tampering, repudiation, information disclosure, denial of service, elevation of privilege