INTERNATIONAL STANDARD

ISO/IEC 20547-4

First edition
2020-09

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

Reference number
ISO/IEC 20547-4:2020(E)

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

5 Overview

5.1 Big data security and privacy concerns

This subclause addresses three types of concerns:

- risks caused by big data characteristics;
- security and privacy challenges from big data;
- ecosystem coordination capabilities needed in the context of big data.

Big data has the key data characteristics of volume, velocity, variety and variability and also the key data processing characteristics of volatility, veracity and value. These characteristics introduce additional risks and thus challenges on the security and privacy aspect of big data.

- Volume of data is at risk associated with massive amounts of data in various layers. For example, multi-tiered, distributed storages and transmission on various networks with different protocols.
- Velocity of data has risks associated with faster flow at which the data is created, stored, analysed or visualized. Security controls can be a burden on velocity and easily omitted.
- Variety of data brings more complexity from a diversity of sources under the control of various actors. Complexity inevitably leads to vulnerability. An emergent phenomenon introduced by big data variety is its ability to infer identity from anonymized datasets by correlating with apparently innocuous public databases.
- Variability of data has risks associated with faster changes in data rate, format/structure, semantics and/or quality. It can become more difficult to apply security controls on data security and privacy.
- Volatility of data can affect to keep audit trails and make security management difficult.
- Veracity of data brings higher requirements to integrity, consistency and accuracy. Associated risks can be aggregated and magnified.
- Value of data brings more attacks for a variety of purposes and interests.

Big data application boom brings more serious security and privacy issues on data, such as frequent incidents of data loss and personal data leakage, illegal data transactions underground, which cause data abuse and Internet fraud and endanger social stability and national security.

From technology platform perspective, due to the continuous emergence of a variety of big data technology, new technical architecture and support platforms and big data software, the following security and privacy capabilities are needed in the big data context.

- Traditional security controls in big data context are needed.

  Massive, multi-sourced, heterogeneous, dynamic and other big data characteristics lead to the difference of data application security from a closed environment. Big data applications generally use open distributed computing and storage architecture with complex underlying support to provide massive data distributed storage and high-performance computing services. These new technologies and architectures make the network boundaries of big data applications become blurred so that the boundary-based traditional security protection measures are no longer valid. Meanwhile, under this new situation, the advanced persistent threat (APT), distributed denial of service (DDoS), machine learning-based data mining and privacy discovery and other attacks make the traditional defence, detection and other security controls expose serious deficiencies. For instance, providing secure data management and threat intelligence, providing secure data storage for big data as well as secure log data generation, transmission, storage, analysis and disposal becomes very difficult. Additionally, novel technical approaches for privacy-preserving, machine learning, cryptographic mechanisms for data-centric security and access control are necessary.

For more information on the requirements of big data security and privacy, refer to the security and privacy technical considerations in different use cases provided by ISO/IEC TR 20547-2.

— Security and privacy need to be provided for the distributed computation and data store infrastructure of big data.

This requires privacy-preserving and secure distributed computation and information dissemination. Big data requires scalable and distributed solutions for secure data storage as well as for audits and investigations for data provenance. Data integrity for streaming influx of data from various sensors and other endpoints has to be provided. Real-time analytics for threat intelligence requires the processing of large amounts of security-related information such as traffic streams and log information.

— Platform security mechanisms need to be improved in the context of big data security and privacy.

In general, existing big data applications use big data management platforms and technology, such as Hadoop-based HBase/Hive, Cassandra/Spark, MongoDB. At the beginning of design, these platforms and technology are mostly considered to be used in the trusted internal network, with little consideration of authentication, authorization, key services and security audit. Although some software is improved, such as adding the Kerberos authentication mechanism, the overall security capability is still relatively weak. Meanwhile, third-party open-source components are often used in big data applications. Due to the lack of rigorous test management and security certification of these components, the ability to prevent software vulnerabilities and malicious backdoors in big data applications is insufficient.

— Application access control capabilities in big data context are needed.

Because of the variety of data types and the wide range of applications of big data, it is often used to provide multiple services to users with different identities and purposes from different organizations or departments. In general, access control is an effective means to achieve controlled access to data. However, due to a large number of unknown data users and data to be accessed, it is very difficult to pre-set roles and permissions of data access. Although the user's rights to access data can be classified in advance, because of the numerous roles, it is difficult to define the control of each role's actual permissions in a fine-grained way. So, it is difficult to accurately specify the range of data for each user to access without deploying a newer access control model such as attribute-base access control (ABAC). This also causes the issue with the data minimization principle in ISO/IEC 29100.

— Scalable security and privacy mechanisms are needed.

When designing and applying security and privacy mechanisms such key management, identity and access management, de-identification, etc., in the big data environment, not only the security and privacy functionalities need to be considered, but also the scalability of these mechanisms needs to be taken into account in order to support processing of high volume and high velocity of the data.

From the data application perspective, due to the big Vs (volume, variety, velocity and variability) characteristics of big data and huge value in big data, the following security and privacy capabilities are needed in big data context:

— Data protection capabilities in big data context are needed.

In the open network society, the huge volume of big data with immeasurable potential value makes it more favoured and easier to become a significant target of network attacks. In recent years, information security incidents frequently occur, for example, leakage of email accounts, social security information and bank card numbers. The distributed system deployment, the open network environment, the complex data application and the large number of user accesses, all cause the big data to face the bigger challenges in confidentiality, integrity, availability and so on.

— Personal data protection capabilities in big data context are needed.

  Due to the large amount of personal data in big data systems, when the security incidents such as data abuse, internal theft and network attacks occur, the consequences of personal data leakage are more serious than ordinary information systems. On the other hand, the advantage of generating value from the analysis and usage of large amounts of data can be compromised by the more risk of personal data leakage during the comprehensive analysis of multi-source data where analysts are easier to explore more personal data through correlation analysis.

— Data authenticity capabilities in big data context are needed.

  Data in big data systems have a wide range of sources that can be a variety of sensors, active uploads and public websites. In addition to reliable data sources, there are a large number of untrusted data sources. Some attackers even deliberately falsify data in an attempt to induce data analysis results. Therefore, it is very important to verify the authenticity of data and their sources. However, there are many difficulties in verifying all the data authenticity because of the performance limitation of data acquisition terminals, the lack of technology, the limited amount of information and the variety and complexity of sources.

— Data owner's right protection capabilities in big data context are needed.

  During the application of big data, the data can be accessed by a variety of users, flow from one controller to another and even be mined to produce new data. Therefore, in the process of data exchange and sharing, there is the circumstance where the data ownership of a data owner and the data use right of a data manager are separated, which implies that data can be out of data owner's control and brings the risks such as data abuse, vague ownership of data, unclear responsibilities of data security supervision so that the rights and interests of data owners can be seriously damaged.

Big data involves ecosystems, or networks of organizations that collaborate to collect, analyse and share data. The following collaborations are needed in a big data context:

— collaboration between stakeholders to ensure that overall ecosystem security and privacy requirements and individual organization's security and privacy requirements are consistent;

— collaboration between stakeholders to ensure that the overall ecosystem risk management and the individual organization's risk management are consistent; and

— collaboration between stakeholders to ensure that individual organizations ensure consistent treatment of the assets to protect.

5.2 Security and privacy objectives

Big data applications have security and privacy objectives. Table 1 describes examples of security objectives. Table 2 describes examples of privacy objectives. Note that Table 2 describes alternative ways to look at objectives.

Table 1 — Security objectives

Objective		Description	Examples
Security protection goals [From ISO/IEC 27000]	Confidentiality	Ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.	Protected transmission of collected data, protected access with suitable authentication schemes, protected processing of data and protected storage.
	Integrity	Ensures the accuracy and completeness of data over its entire life cycle.	Protection of integrity during transmission, processing of data, as well as at storage level using schemes such as digital signatures.
	Availability	Ensures accessibility and usability upon demand by an authorized entity	Preventing service disruptions due to power outages, hardware failures, or denial of service attacks using schemes such as redundant systems.

Table 2 — Privacy objectives

Objective		Description
Privacy principles [From ISO/IEC TR 27550]	Consent and choice	Providing PII principals with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice and to give consent in relation to the processing of their PII at the time of collection
	Purpose legitimacy and specification	Presupposing that the purpose(s) is in compliance with applicable law and relies on a permissible legal basis
	Collection limitation	Limiting the collection of PII to that which is within the bounds of applicable law and strictly necessary for the specified purpose
	Data minimization	Strictly minimizes the processing of PII
	Use retention and disclosure limitation	Limiting the use, retention and disclosure (including transfer) of PII to that which is necessary in order to fulfil specific, explicit and legitimate purposes
	Accuracy and quality	Ensuring that the PII processed is accurate, complete, up to date (unless there is a legitimate basis for keeping outdated data), adequate and relevant for use
	Openness, transparency and notice	Providing PII principals with clear and easily accessible information about the PII controller's policies, procedures and practices concerning the processing of PII
	Individual participation and access	Giving PII principals the ability to access and review their PII, provided their identity is first authenticated with an appropriate level of assurance and such access is not prohibited by applicable law
	Accountability	The processing of PII entails a duty of care and the adoption of concrete and practical measures for its protection
	Information security	Protecting PII under its authority with appropriate controls at the operational, functional and strategic level to ensure the integrity, confidentiality and availability of the PII and protect it against risks such as unauthorized access, destruction, use, modification, disclosure or loss throughout the whole of its life cycle;
	Privacy compliance	Verifying and demonstrating that the processing meets data protection and privacy safeguarding requirements by periodically conducting audits using internal auditors or trusted third-party auditors

Table 2 *(continued)*

Objective		Description
Privacy protection goals [From ISO/IEC TR 27550]	Unlinkability	Ensures that a PII principal may make multiple uses of resources or services without others being able to link these uses together EXAMPLE A customer uses two different accounts for a service that involves big data analysis.
	Transparency	Ensures that an adequate level of clarity of the processes in privacy relevant data processing is reached so that the collection, processing and use of the information can be understood and reconstructed at any time EXAMPLE Understandable documentation covering technology, organization and responsibilities accessible to the PII principal.
	Intervenability	Ensures that PII principals, PII controller, PII processors and supervisory authorities can intervene in all privacy-relevant data processing EXAMPLE Processes for influencing or stopping the data processing fully or partially, manually overturning an automated decision, data portability precautions.
Privacy engineering objectives [From ISO/IEC TR 27550]	Predictability	Providing a reliable understanding of what is occurring with PII processing within a system EXAMPLE Developing a PII processing capability that is repeatable. Related to the transparency protection goal.
	Manageability	Administration of PII with sufficient granularity so that the right level of control can be applied EXAMPLE Development of a privacy preference management that allows PII principal the right level of control. Related to the intervenability protection goal.
	Disassociability	Actively protect or "blind" an individual's identity or associated activities from unnecessary exposure during transactions EXAMPLE Development of a health data processing capability that is anonymous. Related to the unlinkability protection goal.

Clauses 6 to 8 are under the context of big data systems that have the above security and privacy (S&P) concerns and objectives.

Big data security and privacy (BD-S&P) shall be based on the big data reference architecture (BDRA) defined in ISO/IEC 20547-3.

6 Security and privacy aspects of BDRA user view

6.1 Governance activities

6.1.1 Purpose

The data governance defined in ISO/IEC 20547-3 is the governance of an organization that focuses on the data aspect of the organization. The purpose of BD-S&P governance activities is to establish and maintain BD-S&P's coherence and alignment with objectives and constraints with respect to the current and future security and privacy needs of an organization and its stakeholders or interested parties.

NOTE Governance of BD S&P can apply to an organization internally, or to an ecosystem. For instance, an organization in charge of a big data market place can provide governance policies to its participants.

6.1.2 Prepare for and plan BD-S&P governance effort

a) Establish BD-S&P strategy derived from organizational objectives, strategy and vision.

b) Establish role, responsibilities, accountabilities, authorities and organizational structures to support BD-S&P governance effort and reporting requirements.

c) Establish BD-S&P governance organizational structure that is consistent with defined roles, authorities, responsibilities and accountabilities.

d) Establish guiding principles and work instructions for performing BD-S&P governance.

NOTE These work instructions delineate the steps to be performed by those who execute the governance activities. This is to ensure the decision processes are transparent and consistently followed. Sometimes, a secretariat is used to administer these work instructions and to ensure they are properly followed.

e) Establish decision forums to carry out BD-S&P governance work instructions.

f) Define procedures for identifying, managing, auditing and disseminating information related to BD-S&P governance decisions.

1) Link these procedures to BD-S&P strategy.

2) Map these procedures to resources and constraints to support strategy, planning and decision making.

g) Plan BD-S&P governance effort.

1) Establish the scope of BD-S&P governance effort.

2) Establish metrics for BD-S&P governance effort.

3) Identify the data and information needed for BD-S&P governance effort.

4) Identify and define BD-S&P governance work elements and associated resources.

5) Develop BD-S&P governance schedule and define associated milestones.

h) Obtain necessary approvals and funding for the plan.

i) Collect the data and information needed for BD-S&P governance effort.

6.1.3 Monitor, assess and control BD-S&P governance activities

a) Monitor and assess metrics for BD-S&P governance effort.

b) Identify and assess risks and opportunities associated with BD-S&P governance effort.

c) Ensure that other processes (e.g. enterprise life cycle processes, system life cycle processes) are properly using BD-S&P governance directives and guidance.

d) Report BD-S&P governance activity plans and status in accordance with reporting requirements.

e) Assess and control BD-S&P governance effort.

f) Manage risks associated with BD-S&P governance.

6.1.4 Establish BD-S&P governance objectives

a) Examine current and future big-data-related business needs when known.

1) Examine current and future big-data-related enterprise objectives that need to be achieved, such as maintaining a competitive advantage.

   2) Examine and make a judgment on the current and future big-data-related enterprise vision, including strategies, proposals and supply arrangements (whether internal, external, or both) in support of the big-data-related enterprise objectives.

      NOTE 1 The examination can consider the external or internal pressures acting on the enterprise, such as business change, technological change, economic and social trends and political influences.

   3) Examine BD-S&P objectives of the strategies and proposals that are being evaluated.

b) Examine current and future big-data-related mission needs for those missions supported by the enterprise.

   1) Examine current and future big-data-related mission objectives that need to be achieved.

   2) Examine and evaluate possible future use of big data, including strategies, proposals and supply arrangements (whether internal, external or both) in support of the mission objectives.

      NOTE 2 The examination can consider the external or internal pressures acting on the enterprise, such as technological change, economic and social trends and political influences.

   3) Examine BD-S&P objectives of the strategies and proposals that are being evaluated.

c) Establish BD-S&P strategy by making the relevant decisions about the governance in BD-S&P.

   1) Discover, develop, define and evaluate the overall goals of BD-S&P as a whole.

      a) Identify work to be performed to achieve these goals.

      b) Create a configuration of resources that are necessary ingredients in meeting these goals.

      c) Establish a means of measuring governance effectiveness.

   2) Define BD-S&P governance policies related to BD-S&P.

   3) Define a set of governance principles that apply to BD-S&P.

   4) Determine adherence of objectives based on governance compliance criteria and strategies.

   5) Establish management criteria for control of BD-S&P governance practices, dispensations and compliance.

d) Identify BD-S&P objectives to be pursued and desired levels of achievement for each.

6.1.5 Direct BD-S&P

a) Establish and issue governance direction in the form of directives and guidance for BD-S&P.

   1) Develop and issue governance directive(s) that drive the appropriate evolution of BD-S&P.

   2) Implement a governance framework that supports this governance directive to define conceptual and organizational structures and provide a structured decision-making approach.

   3) Establish a decision-making mechanism that minimizes or avoids potential conflicts of interests with an escalation in the enterprise if the problems cannot be properly addressed by BD-S&P governance.

b) Assign responsibility for, direct preparation and implementation of directives, standards and policies that set the direction for BD-S&P efforts.

c) Make strategic decisions within the scope of BD-S&P governance responsibilities and authorities.

d) Review and communicate the decisions.

6.1.6 Monitor and assess compliance with BD-S&P governance directives and guidance

a) Monitor the governance of BD-S&P by the enterprise by utilizing appropriate means.

NOTE 1 BD-S&P is not monitored. In order to see how well BD-S&P are helping to achieve the enterprise goals and objectives, BD-S&P governance can monitor metrics from the development and use of actual entities based on BD-S&P.

b) Establish a means for monitoring compliance with BD-S&P governance directives and guidance.

NOTE 2 A dashboard is a common way of doing this.

c) Presuppose that BD-S&P is in compliance with external obligations (regulatory, legislative, common law, contractual) and internal work practices.

d) When appropriate, BD-S&P governance authority may access directly an entity constructed according to a BD-S&P design under auspices of the governance authority.

NOTE 3 This access by governance is to enable verification that a system, an enterprise, a software item, a service, or other kinds of BD-S&P entity conform to obligations established by governance directives. Merely checking BD-S&P for conformance can be insufficient since BD-S&P features can lack a proper translation into the design or operation of the entity.

e) Establish a responsibility matrix to ensure responsibilities are appropriately assigned.

f) Monitor management plans and status and assess compliance with governance directives and guidance for BD-S&P.

g) Examine the effectiveness of the governance policies and initiate steps to revise the policies as necessary.

h) Collect lessons learned regarding BD-S&P governance as reported from previous engagements and make these lessons available to future projects.

6.1.7 Review implementation of BD-S&P governance directives and guidance and prepare for change

NOTE This activity includes the tasks necessary for the BD-S&P governance authority to close out BD-S&P governance effort.

a) Review all information to assert that BD-S&P governance work is complete and that BD-S&P objectives have been met.

b) Presuppose compliance with current regulations and standards that affect BD-S&P governance.

c) Establish procedures to investigate and capture the various reasons for non-implementation of governance directives and guidance.

d) Record lessons learned and communicate with all relevant stakeholders.

   1) Contribute to best practices for BD-S&P governance.

   2) Scrutinize the effectiveness of governance directives and guidance.

e) Identify and select the changes to be made to BD-S&P governance directives and guidance.

f) Incorporate the changes into BD-S&P governance directives and guidance.

6.2 Management activities

6.2.1 Purpose

The purpose of BD-S&P management activities is to ensure the proper implementation of BD-S&P governance directives and the timely and efficient achievement of BD-S&P objectives.

6.2.2 Prepare for and plan BD-S&P management effort

a) Identify BD-S&P management approaches, constraints, methods, tools and techniques according to BD-S&P governance policies, directives and guidance.

NOTE Management by objectives, management by measurement and management by policies are examples of management approaches.

b) Develop a charter for the management of BD-S&P.

1) Identify organizational assets (people, resources, processes) that influence the management of BD-S&P.

2) Identify knowledge assets (historical information, issues and defect resolutions, successful outcomes) that can aid in the management of BD-S&P.

3) Identify internal and external factors and criteria that influence the management of BD-S&P.

4) Identify in-scope and out-of-scope items that influence the management of BD-S&P.

5) Develop a statement of work in alignment with the charter for management of BD-S&P.

6) Define measurable BD-S&P management objectives and related success criteria for BD-S&P.

c) Develop BD-S&P management organizational structure.

1) Identify the necessary managerial roles, responsibilities and authorities that are concerned with or involved in BD-S&P management.

2) Define a BD-S&P management control hierarchy corresponding to the identified roles and responsibilities.

3) Ensure proper delegation of management responsibilities in the BD-S&P management control hierarchy.

4) Ensure proper allocation of roles to identified role players in the BD-S&P management hierarchy.

d) Plan the effort for managing BD-S&P.

1) Establish the scope of the BD-S&P management effort.

2) Identify metrics for the BD-S&P management effort.

3) Collect the data and information needed for the BD-S&P effort.

4) Obtain access to enablers needed for the BD-S&P management effort.

5) Identify and define BD-S&P management work elements and associated resources.

6) Develop BD-S&P management schedule and define associated milestones.

7) Obtain necessary approvals for the BD-S&P management plan.

8) Ensure that BD-S&P is established and maintained in accordance with the relevant plans.

6.2.3 Monitor, assess and control the architecture management activities

a) Report BD-S&P management activity plans and status.

b) Monitor and assess whether BD-S&P governance directives and guidance are being followed.

c) Monitor and assess metrics for the BD-S&P management effort.

d) Identify and assess risks and opportunities associated with the BD-S&P management effort.

e) Ensure that other processes (e.g. enterprise life cycle processes, system life cycle processes) are properly using BD-S&P management work instructions.

f) Report BD-S&P management activity plans and status in accordance with reporting requirements.

g) Assess and control BD-S&P management effort.

h) Manage risks associated with BD-S&P management.

6.2.4 Develop BD-S&P management approach

a) Develop BD-S&P management plans in accordance with governance directions for BD-S&P.

   1) Identify BD-S&P requirements and other concerns.

   2) Define BD-S&P management scope statement (scope description, acceptance criteria, deliverables, exclusions, constraints, assumptions).

   3) Establish specific BD-S&P management goals that address BD-S&P objectives and specify the reasons for their sufficiency.

   4) Prioritize the goals in terms of their importance in achieving BD-S&P objectives.

   5) Create a work definition that provides a common framework for the overall planning and control of BD-S&P.

      a) Outline the tasks (i.e. the course of action) required for achieving the BD-S&P management goals and order the tasks in terms of importance toward achieving those goals.

      b) Define organizational resources necessary for carrying out the tasks.

      c) Establish evaluation methods for assessing the progress of the tasks towards goal completion.

      d) Identify alternate courses of action (contingency plan) in case certain goals prove to be unattainable.

      e) Ensure that the work definition is consistent with the BD-S&P management goals and includes anticipated levels of uncertainty and change.

   6) Establish the resources necessary for performing the BD-S&P management work elements and assign responsibility and authority to the management hierarchy.

      Develop the resource definition that is essential for delivering the outcomes.

   7) Define management measures that allow assessment of compliance with the BD-S&P management goals.

      Define measurement systems that can aid in the measurement of BD-S&P activities.

b) Develop BD-S&P management schedule in accordance with the BD-S&P management plan(s).

   1) Develop a budget to create and manage BD-S&P and incorporate checks and balances to validate the budget.

2) Develop the schedule for the activities identified in the work definition and define precise and measurable milestones.

3) Define the organizing logic and order of the activities and resources necessary for creating and managing BD-S&P.

4) Estimate the duration of each of the activities and include them as part of the schedule.

c) Adapt the BD-S&P management plan according to new information.

1) Adjust management activities, schedule, directions and goals in response to new information.

2) Prepare adaptive management actions that respond to new problems or opportunities.

3) Apply new knowledge, insights and technologies that contribute to achieving BD-S&P management objectives.

6.2.5 Perform management of BD-S&P

a) Establish and issue management direction in the form of instructions and guidance for BD-S&P.

b) Assign resources to all the identified roles in accordance with the sequence of tasks that needs to be performed.

c) Activate the necessary tracking systems which can capture work performance information and use it to control BD-S&P development.

d) Perform the tasks defined in the BD-S&P management plan to achieve the BD-S&P objectives.

e) Assess BD-S&P management measures, work performance information, resource utilization, probable risks and new opportunities and manage changes to improve work performance.

f) Provide relevant information to all stakeholders as outlined in the BD-S&P management plan.

g) Continually confirm that work performance results conform to the BD-S&P requirements including deviations and dispensations.

h) Set tactical directions for BD-S&P that address policy decisions.

i) Establish individual plans for the development or revision of BD-S&P.

j) Manage decisions about BD-S&P.

k) Manage risks associated with BD-S&P management.

l) Manage changes to BD-S&P.

6.2.6 Monitor BD-S&P effectiveness

a) Monitor and control work performance by tracking, reviewing and regulating the progress to meet the management objectives as per the BD-S&P management plan.

1) Monitor work performance to identify variances from the BD-S&P management plan.

2) Monitor management issues and recommend preventive action in anticipation of possible problems.

3) Monitor management plan execution progress against the schedule estimates.

4) Monitor the health of BD-S&P (using the identified management measures) and identify any areas that require additional attention.

5) Monitor the status of the BD-S&P scope and manage changes to the scope baseline.

   6) Monitor the status of the BD-S&P management schedule and manage changes to the schedule baseline.

b) Assess actual outcomes against planned targets and make corrective actions when necessary.

c) Collect and communicate performance information to all relevant stakeholders at periodic intervals.

   1) Maintain accurate and timely information concerning BD-S&P.

   2) At periodic intervals, assess whether the BD-S&P management objectives are being reached.

   3) Provide forecasts to update current schedule information.

d) Define quality assurance actions and audits that confirm the execution of the BD-S&P management plans.

e) Report BD-S&P management activity plans and status in accordance with reporting requirements.

f) Assess and control the BD-S&P management effort.

6.2.7 Update the BD-S&P management plan

a) Finish the previous BD-S&P management plan.

b) Review all information to assert that the BD-S&P management work is complete and that the BD-S&P objectives have been met.

c) Monitor and assess metrics for the BD-S&P management effort.

d) Presuppose compliance with regulations and standards that affect BD-S&P.

e) Establish procedures to investigate and capture the various reasons for management actions taken as part of BD-S&P management.

f) Record lessons learned and communicate to all relevant stakeholders.

   1) Contribute to best practices for BD-S&P management.

   2) Scrutinize the effectiveness of management approaches that were adopted in order to address the BD-S&P management problem.

g) Identify changes to be made to the BD-S&P management plan.

h) Select the changes to be made in the next iteration of the BD-S&P management plan.

i) Incorporate the changes into the BD-S&P management plan.

6.3 Operation activities

6.3.1 BD-S&P solution design activities

6.3.1.1 Purpose

The purpose of BD-S&P solution design activities is to identify BD-S&P solutions that address stakeholder concerns, achieve BD-S&P objectives and meet relevant requirements.

NOTE 1 An important aspect of BD-S&P solution design is to allow the analysts and stakeholders to understand the trade space of potential options that can meet the objectives (see 6.3.1.7 for more information on the nature of a trade space). Typically, a varied and distinctive mix of BD-S&P solutions is considered in order to allow the trade-off between various constraints and concerns. In other words, in dealing with a complex problem space, a full exploration of the solution space is necessary as part of the BD-S&P solution design activities to eventually select the most appropriate solution.

NOTE 2 The candidate BD-S&P solution(s) can be derived from or can be already existing BD-S&P solution(s) under BD-S&P management oversight or from other sources.

6.3.1.2 Prepare for and plan the BD-S&P solution design effort

a) Identify the potential problem area(s) that need to be addressed.

b) Define the expected purpose, scope, objectives and level of detail of the BD-S&P solution design effort.

c) Define one or more BD-S&P solution design approaches that are consistent with the BD-S&P governance and management directions and are consistent with the purpose, scope and objectives of this effort.

d) Select or develop the requisite techniques, methods and tools for BD-S&P solution design.

e) Plan the BD-S&P solution design effort.

   1) Establish the scope of the BD-S&P solution design effort.

   2) Establish metrics for the BD-S&P solution design effort.

      NOTE 1 At a minimum, metrics and criteria that enable the BD-S&P solution design team to determine when the BD-S&P solution design task is complete, is established.

   3) Identify the data and information needed for the BD-S&P solution design effort.

   4) Obtain access to enablers needed for the BD-S&P solution design effort.

      NOTE 2 The enablers are usually obtained from the BD-S&P solution enablement activities. When enablers are obtained from other sources, these can become candidate enablers for use by other projects through the BD-S&P solution enablement activities.

   5) Identify and define BD-S&P solution design work elements and associated resources.

   6) Develop BD-S&P solution design schedule and define associated milestones.

f) Obtain necessary approvals and funding for the plan.

g) Collect the data and information needed for the BD-S&P solution design effort.

h) Ensure personnel is trained in the use of identified techniques, methods and tools.

6.3.1.3 Monitor, assess and control the BD-S&P solution design activities

a) Report BD-S&P solution design activity plans and status.

b) Monitor and assess whether BD-S&P governance directives and guidance are being followed.

c) Monitor and assess whether BD-S&P management instructions and guidance are being followed.

d) Monitor and assess metrics for the BD-S&P solution design effort.

e) Identify and assess risks and opportunities associated with the BD-S&P solution design effort.

f) Maintain traceability of BD-S&P solution design results to the source material used during the activities.

g) Implement corrective actions to modify the work plan or realign the work with the plan.

h) Assess and control the BD-S&P solution design effort.

6.3.1.4 Characterize problem space and associated problems

a) Identify current and projected situation(s) in the problem space.

NOTE 1 The problem space and the solution space are abstract. However, the problem and the solution themselves can be actual or perceived and they can also be tangible or intangible. For example, the problem can be inefficient work (actual or perceived) and the solution can be to use faster machines (tangible) or apply better processes (intangible). In simple terms, the problem space relates to the world of end-user challenges and motivations — it is all about needs (states of felt deprivation). The solution space relates to the world of products, services and technology — it is all about the offerings that satisfy needs.

b) Identify problems, difficulties and opportunities in the current and projected situation(s).

NOTE 2 The concept of "problem" is used here in the same sense used in ISO/IEC/IEEE 15288: "difficulty, uncertainty, or otherwise realized and undesirable event, set of events, condition, or situation that requires investigation and corrective action". A problem space is a mental representation of a problem (or set of problems) that contains the knowledge of the initial state and the goal state of the problem(s) as well as possible intermediate states that need to be searched in order to link up the beginning and the end of the task.

c) Identify relevant aspects of the identified situation(s).

NOTE 3 An aspect is a way in which a thing can be viewed or regarded, an interpretation, or a different viewpoint. A clear understanding of the different aspects involved can help ensure that the full nature of the problems, difficulties and opportunities are well understood. It is a common error to not consider these things from different perspectives.

d) Examine current and future business and mission need with respect to these problems, difficulties and opportunities.

e) Identify stakeholders and their concerns corresponding to each of these problems, difficulties and opportunities.

f) Identify and analyse any formal and informal requirements that apply to this situation and document which requirements are relevant to current effort and how they would flow to the evaluation criteria.

g) Identify quality attributes associated with these stakeholder concerns.

h) Identify and characterize how the problems, difficulties and opportunities affect different stakeholders and their priorities in addressing these items.

i) Identify and characterize complexities of each problem, difficulty and opportunity, its cause and effect and how it is being addressed currently in each of the identified situations.

6.3.1.5 Establish BD-S&P solution objectives and evaluation criteria

a) Gather, analyse and negotiate relevant requirements for each identified problem, difficulty and opportunity.

b) Determine boundary conditions, root causes, drivers and relevant scenarios for each identified problem, difficulty and opportunity.

c) Determine gaps or shortfalls of current or planned solutions in addressing the problem.

d) Identify relevant assumptions, degrees of freedom, constraints, conditions and challenges.

e) Identify and characterize the cause and effect relationships for the identified problem(s) or difficulties.

EXAMPLES Inference networks can be used to characterize cause-effect relationships and can take various forms depending on the situation such as, for example, problem tree, influence diagram, Bayesian network, causal loop diagrams, fishbone diagrams, etc.

f) Formulate a clear statement of the problem(s) and opportunity(ies).

g) Identify and define BD-S&P solution objectives that address the problem(s) concerning the stakeholder concerns, requirements, or quality attributes, or that take advantage of identified opportunities.

h) Define evaluation criteria that can be used to assess the extent to which the problems(s) are resolved and to inform exploration and selection of alternatives.

NOTE These evaluation criteria are directly related to aspects of the problem(s) in the problem space and are primarily concerned with achieving desired "ends." As such, these are sometimes called ends objectives. In some domains, the ends objectives are related directly to desired "effects" and are the basis for so-called effects-based analysis. These criteria are different but related to the "means objectives" to be defined during solution space analysis.

6.3.1.6 Synthesize potential solution(s) in the solution space

a) Develop an objective view by reformulating the elements in the cause-effect characterization as conditions and levels to be achieved in addressing the problems revealed by examination of this characterization.

b) Identify problem mitigation strategies that can achieve those conditions and levels and serve as a potential solution(s).

   1) Perform technology scan for relevant technologies.

   2) Perform problem/solution pattern scan for relevant solutions to similar problems.

   3) Perform natural system metaphor scan for possible naturally occurring solutions to similar problems.

   4) Perform risk assessment of the identified strategies.

c) Identify existing or previous solutions to determine if these can be used as a potential solution(s) for the current or projected situation under examination.

NOTE 1 Solutions can be found in current or future BD-S&P solutions and can sometimes address more than one problem or difficulty.

d) Review the resulting relationships between problem mitigation strategies and problem causes to assure the completeness of the potential solution(s).

NOTE 2 Strategies can apply to multiple objectives. It can be important to specify the relationships between strategies and objectives to facilitate the examination of solution completeness.

e) Formulate purpose statement(s) for each potential solution.

NOTE 3 There can be a different purpose statement for each solution since the solution may not be addressing the entire problem or all aspects of the problem.

f) Identify needs, wants and expectations for each potential solution.

NOTE 4 Expectations are what someone regards as likely to happen, which can have nothing to do with what they need or want. Expectations can drive the solutions as much as what can be needed or wanted by a person.

g) Identify relevant critical success factors and key performance indicators for each potential solution.

NOTE 5 Success factors can be different for each potential solution. It depends on the problem perspective on which the solution is based. Success factors are relative to the purpose of that particular solution. The proposed solutions can also be addressing different aspects/parts of the problem. Success factors and performance indicators can be based on the identified stakeholder concerns or quality attributes from problem space analysis.

6.3.1.7 Characterize solutions and the trade space

NOTE 1 Trade space is the range and extent of parameters, properties and characteristics required to satisfy BD-S&P solution objectives and stakeholder concerns. Trade space analysis is used for analysing the relevant constraints, conditions and challenges involved in large complex problems with multiple stakeholders and multiple objectives. It involves the identification and understanding of trade-offs involved in choosing between competing solutions.

a) Examine the context in which stakeholders perceive value and formulate value propositions for each potential solution.

b) Identify strengths, weaknesses, opportunities and threats for each potential solution.

c) Identify other important aspects related to each potential solution including, but not limited to, the following.

   1) Identify and characterize risks for each potential solution.

   2) Identify assumptions with respect to each potential solution.

   3) Identify additional problems that can be caused by each potential solution.

   4) Determine remaining gaps or shortfalls after implementing the proposed solutions.

d) Harmonize elements of each potential solution to ensure that it can be realized in a coherent and cohesive manner.

e) Identify and characterize the trade-offs between and within proposed solutions.

NOTE 2 Trade-offs can be within each solution and between solutions. There are also trade-offs between proposed solutions and the status quo (which can be considered as one of the alternative “solutions” to be considered). Typical trade-offs to consider are the following: cost vs performance, cost vs schedule, weight vs speed, accuracy vs timeliness, acquisition cost vs operating cost, ease of use vs security, flexibility vs predictability, agility vs robustness, risk vs reward, etc.

f) Identify and characterize negative and positive influences and interactions between proposed solutions and pre-existing/planned solutions.

g) Formulate a roadmap for implementing the proposed solution(s).

h) Define evaluation criteria that can be used to assess the extent to which the proposed solution(s) address the specified problem(s) and to inform exploration and selection of alternatives.

NOTE 3 These evaluation criteria are directly related to aspects of the solution(s) in the solution space and are primarily concerned with the “means” by which a solution addresses the identified problems. As such, these are sometimes called means objectives. These criteria are different but related to the “ends objectives” defined during problem space analysis.

6.3.1.8 Formulate candidate BD-S&P solution(s)

a) Establish and capture the desired functional and non-functional characteristics based on the potential solution(s) with respect to the purpose of each solution that corresponds to the stakeholder concerns, relevant requirements and constraints and quality attributes identified during problem space analysis.

b) Devise structural, behavioural and organizational concepts and properties that support the desired functional and non-functional characteristics.

EXAMPLE 1 These concepts and properties can be expressed in the form of information-technology-like constructs such as information flows, control flows, data structures, operational rules, event/trace diagrams, state transition diagrams, timelines, roadmaps, etc.

EXAMPLE 2 These concepts and properties can be expressed in other forms such as risk models, financial models, economic models, simulation models, sensitivity models, queuing models (as well as other kinds of continuous and discrete event simulation models), geospatial models, management models, business models, social- and environmental impact models, value stream models, etc.

c) Identify and characterize the trade-offs between candidate BD-S&P solutions.

d) Identify key characteristics that provide insight into the BD-S&P solution and use them to define the context and scope of the BD-S&P solution(s).

NOTE 1 These characteristics are based on identified stakeholder concerns, relevant requirements, quality attributes, BD-S&P solution objectives and other relevant factors. A mapping between such drivers and the characteristics can be developed to aid in traceability.

e) Formulate principles, guidelines, protocols and standards for each candidate BD-S&P solution.

f) Decompose and allocate the characteristics to components and processes that make up each candidate BD-S&P solution.

g) Identify the processes and activities that, when arranged or performed in a specific order, provide or enable the identified characteristics.

h) Identify rules governing the components, their composition, interaction and interdependence that ensure that each candidate BD-S&P solution provides or enables the desired characteristics.

i) Ensure that each candidate BD-S&P solution provides the desired characteristics or enables them to be realizable.

j) Identify issues and areas for improvement in the BD-S&P solution(s).

k) If more than one BD-S&P solution is generated, select the best BD-S&P solution(s) for use downstream.

NOTE 2 The BD-S&P solution evaluation activities can be used to facilitate the selection of the most suitable BD-S&P solution(s). The results of problem space analysis can be used as a basis for the evaluation criteria. Often an initial screening of candidate BD-S&P solutions is conducted prior to sending these for evaluation to avoid unnecessary effort in evaluating candidates that are duplicative, too costly or risky, unsuitable or infeasible, etc.

NOTE 3 Sometimes the selection of the BD-S&P solution(s) going forward is made through decisions outside the scope of the BD-S&P solution design activity. In that case, then the candidate BD-S&P solutions are presented to decision-makers along with an assessment of these BD-S&P solutions.

6.3.2 BD-S&P solution evaluation activities

6.3.2.1 Purpose

The purpose of BD-S&P solution evaluation activities is to determine the extent to which one or more BD-S&P solutions meet BD-S&P objectives and address stakeholder concerns, or to determine the quality or completeness of BD-S&P.

6.3.2.2 Prepare for and plan the BD-S&P solution evaluation effort

a) Identify the potential decision(s) that can be addressed by the BD-S&P solution evaluation effort.

b) Define the expected purpose, scope, objectives and level of detail of the BD-S&P solution evaluation effort.

c) Review stated purpose, scope and objectives of the BD-S&P solution evaluation effort with the sponsor, designer and other interested parties.

d) Define one or more BD-S&P solution evaluation approaches that are consistent with the BD-S&P governance and management directions and are consistent with the purpose, scope and objectives for this effort.

e) Select or develop the requisite techniques, methods and tools for BD-S&P solution evaluation.

f) Select or develop a BD-S&P solution evaluation framework.

g) Collect any relevant regulatory requirements.

h) Plan the BD-S&P solution evaluation effort.

   1) Establish the scope of the BD-S&P solution evaluation effort.

   2) Establish metrics for the BD-S&P solution evaluation effort.

   3) Identify the data and information needed for the BD-S&P solution evaluation effort.

   4) Obtain access to enablers needed for the BD-S&P solution evaluation effort.

   NOTE The enablers are usually obtained from the BD-S&P solution enablement activities. When enablers are obtained from other sources, these can become candidate enablers for use by other projects through the BD-S&P solution enablement activities.

   5) Identify and define BD-S&P solution evaluation work elements and associated resources.

   6) Develop BD-S&P solution evaluation schedule and define associated milestones.

i) Obtain necessary approvals and funding for the plan.

j) Collect the data and information needed for the BD-S&P solution evaluation effort.

k) Ensure personnel is trained in the use of identified techniques, methods and tools.

l) Ensure personnel has necessary and appropriate access to relevant BD-S&P solution work products.

6.3.2.3 Monitor, assess and control the BD-S&P solution evaluation activities

a) Report BD-S&P solution evaluation activity plans and status.

b) Monitor and assess whether BD-S&P governance directives and guidance are being followed.

c) Monitor and assess whether BD-S&P management directives and guidance are being followed.

d) Monitor and assess metrics for the BD-S&P solution evaluation effort.

e) Identify and assess risks and opportunities associated with the BD-S&P solution evaluation effort.

f) Maintain traceability of BD-S&P solution evaluation results to the source material used during the activities.

g) Ensure traceability and integration of assessed information.

h) Implement corrective actions to modify the work plan or realign the work with the plan.

i) Assess and control the BD-S&P solution evaluation effort.

j) Manage risks associated with BD-S&P solution evaluation.

6.3.2.4 Determine evaluation criteria

NOTE 1 The evaluation criteria consist of both the value assessment criteria and the attribute analysis criteria.

NOTE 2 The evaluation objectives can be related to the objectives used in BD-S&P solution design or not. In any case, the design objectives need to be examined to determine to what extent they apply to this evaluation.

NOTE 3 The evaluation criteria can be based on the results of problem space analysis performed during BD-S&P solution design or elsewhere.

a) Identify relevant mandates and imperatives, including relevant policies and standards.

b) Identify relevant stakeholders and their concerns for the BD-S&P solution(s) being evaluated.

NOTE 4 The stakeholder concerns to be considered during the BD-S&P solution evaluation can be different from the stakeholder concerns addressed during the original design of the BD-S&P solution(s). The evaluation, for example, can be tasked with determining if the BD-S&P solution can be suitable for some other purpose than that originally envisioned.

c) Define value assessment criteria that contribute to key success factors, key indicators and decisions that need to be made.

NOTE 5 During BD-S&P solution evaluation, those value assessment criteria defined during BD-S&P solution design can be evaluated for relevance in the evaluation effort and if necessary, additional criteria can be added or existing criteria can be modified to reflect the evaluation context.

d) Define attribute analysis criteria that support the value assessment criteria.

NOTE 6 Consider the agreed quality attributes for the BD-S&P solution as candidates for attribute analysis criteria.

e) Determine value assessment and attribute analysis criteria structure and relationships.

NOTE 7 The relationships between value assessment and attribute analysis criteria is considered when the results of the analysis are used to determine the extent to which stakeholder concerns are addressed. These relationships can often be structured in such a way to facilitate doing the value assessment and correlating this with the analysis results.

f) Determine relationships between value assessment criteria and attribute analysis criteria and elements of value or utility (e.g. value function, utility curve).

NOTE 8 This task determines how the two sets of criteria map to the "value curves" that represent the figures of merit for the BD-S&P solution.

6.3.2.5 Determine evaluation methods and integrate with evaluation objectives and criteria

a) Select or develop value assessment and attribute analysis methods that support the defined value assessment and attribute analysis criteria

NOTE 1 These methods can have been developed by the BD-S&P solution enablement activities. If so, then they are located in the BD-S&P solution repository. If these methods are developed here, then they can be supplied to BD-S&P solution enablement as candidate items to be made appropriate for reuse across the organization.

b) Review assessment and analysis objectives, criteria and methods and associated scales and weights (if any) with the sponsor and designer.

c) Identify sources of information for use during the application of the value assessment and attribute analysis criteria.

NOTE 2 Some information comes from analysis but other information can come from other sources, such as prior evaluation efforts, operational experience, industry databases, system verification activities and research activities.

6.3.2.6 Establish measurement techniques, methods and tools

NOTE 1 Many BD-S&P solution evaluations can be performed adequately without invoking a substantial multi-tiered structure of value assessment and attribute analysis layers. At a minimum, the evaluation assesses each alternative against the criteria. It does not always need to be quantitative and does not always need to apply measurement scales. Weights are not absolutely required since this is nearly always a multi-objective problem and the goal is usually to present to the stakeholders the trade-offs between those objectives, not necessarily to mathematically determine the "best" solution.

a) When appropriate, utilize scales and weight as a means to measure the factors and properties of the BD-S&P solution.

1) Define analysis scales for measuring against the analysis criteria, if appropriate.

2) Define assessment scales for measuring against the assessment criteria, if appropriate.

3) Specify weights for assessment and analysis criteria, if appropriate.

NOTE 2 Some methods do not use weights, while others depend on them to achieve more accurate results. There are different kinds of weights, such as importance weights, swing weights, criticality weights. The methods chosen usually specify the kinds of weights to be used.

4) Determine where on these scales the BD-S&P solution is now and identify the desired point(s) for future levels of achievement.

b) Identify appropriate measures for the relevant BD-S&P solution attributes.

c) Identify metrics to be determined from the measures.

NOTE 3 There is an overlap between measures and metrics. Both can be qualitative or quantitative, but what distinguishes them is important. Measures are concrete, usually measure one thing and are quantitative in nature (e.g. I have five apples). Metrics describe quality and require a measurement baseline (I have five more apples than I did yesterday). Measures and metrics can be useful for setting program priorities, allocating resources and measuring performance.

d) Define relationships between measures, metrics and evaluation criteria.

e) Identify sources of information for obtaining values for these measures and metrics.

f) Identify techniques, methods and tools appropriate for these measures, metrics and evaluation criteria.

g) Estimate the likely accuracy, errors and level of uncertainty in results when using these measures, metrics and evaluation criteria.

6.3.2.7 Review evaluation-related information

a) Identify relevant information for the chosen value assessment and attribute analysis methods.

NOTE 1 If possible, reuse existing data and results from previous evaluations of this kind, if the information available is still valid.

b) Collect all relevant and necessary information.

c) Create additional information if not readily obtainable (i.e. non-existent, inaccessible) and if its creation is feasible within the available time without causing disruptions.

d) Examine and qualify collected artifacts in terms of completeness, correctness and consistency.

e) Develop an understanding of the BD-S&P solution, the BD-S&P solution quality attributes, key decisions and system concerns.

NOTE 2 Quality attributes can be defined to characterize how stakeholder concerns can be addressed.

6.3.2.8 Analyse BD-S&P solution attributes and assess stakeholder value

a) Identify BD-S&P solution alternatives for evaluation, if appropriate.

NOTE 1 The alternatives can come from the BD-S&P solution design activities.

NOTE 2 The status quo is sometimes one of the alternatives to be considered.

NOTE 3 Development of these alternatives can be outside the scope of the evaluation activity. However, sometimes the evaluation activity determines that there is an insufficient number, variety, or extent of alternatives that have been predefined and that additional alternatives need to be generated.

NOTE 4 Eliminate alternatives that are similar to each other and that do not provide a discriminating case with respect to the evaluation criteria.

b) Use the assessment and analysis method(s) as specified in the evaluation work plan to assess the BD-S&P solution for the identified purpose.

c) Use selected evaluation methods to determine the concepts and properties of the BD-S&P solution (alternatives) with respect to the evaluation criteria.

EXAMPLE Examples of methods to determine these concepts and properties include elements such as analysis, observation, simulation, prototyping, experimentation, inspection, audit, review, walk-through and expert judgment.

d) Evaluate the BD-S&P solution or the BD-S&P solution alternatives against the identified quality attributes, stakeholder concerns and BD-S&P solution objectives.

e) Identify and characterize costs, risks and opportunities.

NOTE 5 Risks have been identified during the BD-S&P solution design for each potential solution under consideration. The risks identified here for the BD-S&P solution under evaluation can be related to those solutions risks identified before.

f) Characterize the accuracy of, the levels of uncertainty associated with and the extent of errors in the measurements used and other results obtained during the evaluation.

6.3.2.9 Characterize BD-S&P solution(s) based on assessment results

a) Identify and characterize trade-offs with respect to quality attributes, stakeholder concerns, BD-S&P solution attributes, costs, risks and opportunities.

b) Assess whether and the extent to which, relevant mandates and imperatives, including relevant policies and standards, are met by the BD-S&P solution(s).

NOTE 1 Sometimes the BD-S&P solution meets the objectives and addresses stakeholder concerns but does not meet a mandate or imperative. It can be possible to get relief from meeting such mandates or imperatives, so it is appropriate to examine this possibility.

NOTE 2 It is sometimes better to eliminate BD-S&P solution alternatives that fail to meet mandates and imperatives earlier in the process to avoid expending considerable resources in the further evaluation of these items. However, it can also be helpful to see how far off these are from meeting the mandates and imperatives.

c) Assess results of this analysis to determine, as appropriate, the best BD-S&P solution(s) among the alternatives, the quality of a BD-S&P solution, or the extent to which a BD-S&P solution meets BD-S&P solution objectives, meets relevant requirements, or satisfies stakeholder concerns.

d) Review analysis and assessment results with the sponsor, designer and other interested parties.

6.3.2.10 Formulate findings and recommendations

a) Identify and characterize findings from the evaluation.

b) Analyse the findings.

c) Validate the findings with subject matter experts and other relevant parties.

d) Assess the implications of findings.

e) Develop recommendations.

f) Review findings and recommendations with the sponsor, designer and other interested parties.

6.3.2.11 Capture and communicate evaluation results

a) Identify the audience for communicating the evaluation results.

b) Select the most relevant and elaborate on key findings and recommendations.

c) Develop an evaluation report.

d) Obtain approval for the report, if appropriate.

e) Present findings and recommendations to decision-makers, if relevant.

f) Present to key stakeholders and designers.

g) Capture responses from these presentations (e.g. issues, action items, risks, observations, perspectives).

h) If required or requested, iterate relevant parts of the evaluation.

i) If an evaluation is updated, review changes with the sponsor, designer and other interested parties.

j) Update reports, if necessary, based on feedback from presentations.

k) Archive report and responses received during presentations.

6.3.3 BD-S&P solution enablement activities

6.3.3.1 Purpose

The purpose of BD-S&P solution enablement activities is to develop, maintain and improve the enabling capabilities and resources needed in performing BD-S&P solutions. This can involve the acquisition or development of these capabilities and resources as and when required.

6.3.3.2 Prepare for and plan the BD-S&P solution enablement effort

a) Identify the enabling capabilities and resources needed for support to BD-S&P governance and management.

b) Identify the enabling capabilities and resources needed for support to the design and evaluation of BD-S&P solutions.

c) Identify the guidelines, policies, strategies and constraints for deploying the enabling capabilities and resources.

NOTE These guidelines, policies, strategies and constraints can be obtained from the BD-S&P governance directives and BD-S&P management guidance.

d) Identify and define the necessary roles and responsibilities of people involved in the BD-S&P solution enablement effort.

e) Plan the BD-S&P solution enablement effort.

1) Establish the scope of the BD-S&P solution enablement effort.

2) Establish metrics for the BD-S&P solution enablement effort.

3) Collect the data and information needed for the BD-S&P solution enablement effort.

4) Obtain access to the capabilities and resources needed for the BD-S&P solution enablement effort.

5) Identify and define BD-S&P solution enablement work elements and associated resources.

6) Develop a BD-S&P solution enablement schedule and define associated milestones.

7) Develop necessary control and communication plans for BD-S&P solution enablement.

f) Obtain necessary approvals and funding for the plan.

6.3.3.3 Monitor, assess and control the BD-S&P solution enablement activities

a) Report BD-S&P solution enablement activity plans and status.

b) Monitor and assess whether BD-S&P governance directives and guidance for BD-S&P solution enablement are being followed.

c) Monitor and assess whether BD-S&P management directives and guidance for BD-S&P solution enablement are being followed.

d) Monitor and assess metrics for the BD-S&P solution enablement effort.

e) Identify the enablement issues arising from changes to the BD-S&P solution approach.

NOTE For example, moving from a functional-based to a service-oriented approach can lead to a significant change in the BD-S&P solution enablement items.

f) Identify and assess risks and opportunities associated with the BD-S&P solution enablement effort.

g) Monitor and assess whether BD-S&P solution enablers are being utilized properly.

h) Monitor and assess whether the BD-S&P solution repository and library are being utilized properly.

i) Implement corrective actions to modify the work plan or realign the work with the plan.

j) Assess and control the BD-S&P solution enablement effort.

6.3.3.4 Manage the BD-S&P solution process enablers

a) Manage decisions about BD-S&P solution enablers using the Decision Management process in ISO/IEC/IEEE 15288 as a guide.

b) Manage risks associated with BD-S&P solution enablers using the Risk Management process in ISO/IEC/IEEE 15288 as a guide.

c) Manage changes to the BD-S&P solution process enablers using the Configuration Management process in ISO/IEC/IEEE 15288 as a guide.

d) Manage the BD-S&P solution repositories, libraries and registries using the Information Management process in ISO/IEC/IEEE 15288 as a guide.

e) Manage the BD-S&P solution repositories, libraries and registries using the Knowledge Management process in ISO/IEC/IEEE 15288 as a guide.

f) Manage the quality of BD-S&P solution enablers using the Quality Management process in ISO/IEC/IEEE 15288 as a guide.

g) Manage infrastructure associated with BD-S&P solution enablers using the Infrastructure Management process in ISO/IEC/IEEE 15288 as a guide.

6.3.3.5 Develop and establish enabling capabilities and resources

a) Identify capabilities and resources that can be leveraged for facilitating the achievement of BD-S&P vision, strategy, goals and objectives.

b) Develop a catalogue of capabilities and resources that can be used by the other BD-S&P activities and put this catalogue in the BD-S&P solution registry.

c) Develop and establish a BD-S&P solution repository that can be used to store BD-S&P solution-related information and data.

d) Establish access control measures for the BD-S&P solution-related information and data in the BD-S&P solution repository.

e) Establish work product templates that can be used by the other BD-S&P activities.

f) Develop the requisite information and information flows needed for governing and managing BD-S&P.

g) Identify areas of improvement and additional training to be provided in order to drive the BD-S&P vision, strategy, goals and objectives.

h) Establish services, activities, events and controls that can be applied for BD-S&P solution enablement.

NOTE Events are milestones, reviews, audits, key decision points, quality gates, etc. Controls are checklist, entry criteria, exit criteria, decision trees, etc.

6.3.3.6 Deploy capabilities and resources for use by the other BD-S&P activities

a) Deploy the BD-S&P solution repository for maintaining the BD-S&P solution work-products.

b) Align activities, services, resources, capabilities and information cohesively for the provision of effective BD-S&P solution enablement.

c) Deploy capabilities, services, activities, events and controls for support to the other BD-S&P activities.

d) Deploy the appropriate organizational resources, capabilities, assets, activities and services for the provision of BD-S&P solution enablement.

e) Deploy BD-S&P solution work product templates.

f) Deploy information structures and information flows necessary for BD-S&P solution enablement.

g) Deploy mechanisms to collect relevant data and information needed for the BD-S&P solution enablement effort.

h) Deploy mechanisms to collect relevant data and information needed for managing the BD-S&P solution repository.

i) Provide training and certification on enabling capabilities and resources.

6.3.3.7 Improve BD-S&P solution enablement capabilities and resources

a) Identify gaps and shortfalls in enabling capabilities and resources.

   1) Mechanisms used to collect data and information "related to" or "used in" BD-S&P solution enablement.

   2) BD-S&P solution repository contents and structure.

   3) BD-S&P solution library contents and structure.

   4) BD-S&P solution registry contents and structure.

   5) Work product templates and guidelines.

   6) Information structures and flows related to performing the other BD-S&P activities.

   7) Enablement services, activities, events and controls.

   8) BD-S&P governance enablers.

   9) BD-S&P management enablers.

   10) BD-S&P solution design enablers.

   11) BD-S&P solution evaluation enablers.

b) Examine gaps and shortfalls to identify potential improvements.

c) Propose improvements to the enabler development activity.

d) Monitor the development of the improved enablers to ensure the expected improvements are achieved.

6.4 Security and privacy aspects of big data roles

All roles of big data defined in ISO/IEC 20547-3, including big data application provider (BDAP), big data framework provider (BDFP), big data service partner (BDSP), big data consumer (BDC) and big data provider (BDP) (see ISO/IEC 20547-3:2020, Clause 8) have the responsibility of maintaining big data security and privacy (S&P). As shown in Figure 1, the S&P aspects of big data roles are:

- big data S&P planning;
- big data S&P managing;
- big data S&P implementing;
- big data S&P operating;
- big data S&P auditing.

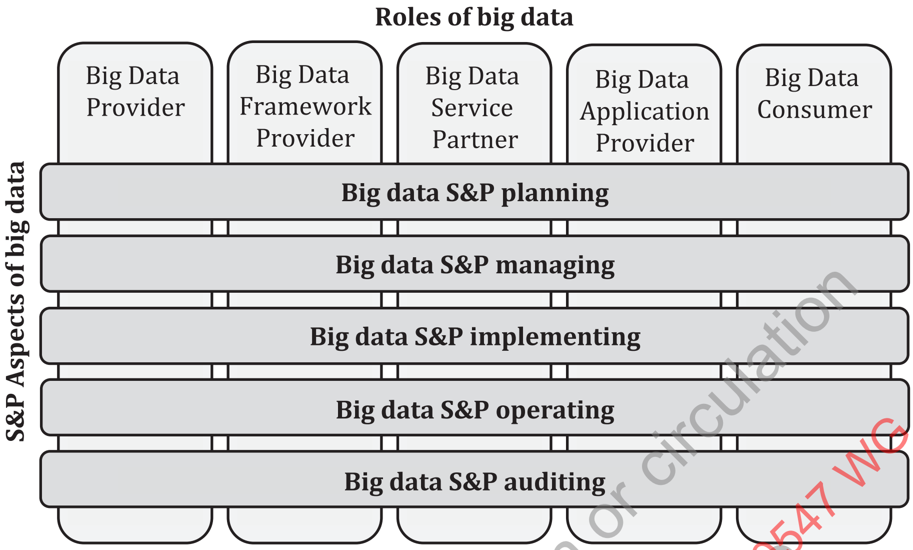

Figure 1 — BDRA-S&P user view

An organization generally has a three-layered structure that consists of the governance layer, management layer and operation layer. Figure 2 shows the positions of big data S&P aspects in the three-layered structure.

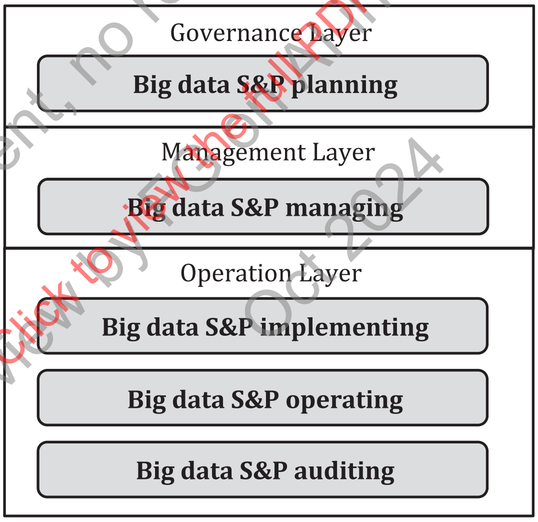

Figure 2 — Big data S&P aspects in organizational three-layered structure

The governance activities described in 6.1 are mapped to big data S&P planning. The management activities described in 6.2 are mapped to big data S&P managing. The operation activities described in 6.3 are mapped to big data S&P implementing, big data S&P operating and big data S&P auditing. Table 3 shows big data S&P aspects and their activities according to these mappings.

Table 3 — Big data S&P aspects and their activities

S&P aspects	Sub-clause	Activities	Purpose
Big data S&P Planning	6.1.2	Prepare for and plan big data S&P governance effort	To establish and maintain BD-S&P's coherence and alignment with objectives and constraints with respect to the current and future security & privacy needs of an organization and its stakeholders or interested parties
	6.1.3	Monitor, assess and control big data S&P governance activities	
	6.1.4	Establish big data S&P governance objectives	
	6.1.5	Direct big data S&P	
	6.1.6	Monitor and assess compliance with big data S&P governance directives and guidance	
	6.1.7	Review implementation of big data S&P governance directives and guidance and prepare for change	
Big data S&P Managing	6.2.2	Prepare for and plan big data S&P management effort	To ensure the proper implementation of BD-S&P governance directives and the timely and efficient achievement of BD-S&P objectives
	6.2.3	Monitor, assess and control the architecture management activities	
	6.2.4	Develop big data S&P management approach	
	6.2.5	Perform management of big data S&P	
	6.2.6	Monitor big data S&P effectiveness	
	6.2.7	Update the BD-S&P management plan	
Big data S&P Implementing	6.3.1.2	Prepare for and plan the BD-S&P solution design effort	To identify BD-S&P solutions that address stakeholder concerns, achieve BD-S&P objectives and meet relevant requirements
	6.3.1.3	Monitor, assess and control the BD-S&P solution design activities	
	6.3.1.4	Characterize problem space and associated problems	
	6.3.1.5	Establish BD-S&P solution objectives and evaluation criteria	
	6.3.1.6	Synthesize potential solution(s) in the solution space	
	6.3.1.7	Characterize solutions and the trade space	
	6.3.1.8	Formulate candidate BD-S&P solution(s)	
Big data S&P Operating	6.3.3.2	Prepare for and plan the BD-S&P solution enablement effort	To develop, maintain and improve the enabling capabilities and resources needed in performing BD-S&P solutions.
	6.3.3.3	Monitor, assess and control the BD-S&P solution enablement activities	
	6.3.2.4	Manage the BD-S&P solution process enablers	
	6.3.3.5	Develop and establish enabling capabilities and resources	
	6.3.3.6	Deploy capabilities and resources for use by the other BD-S&P activities	
	6.3.3.7	Improve BD-S&P solution enablement capabilities and resources	
Big data S&P Auditing	6.3.2.2	Prepare for and plan the BD-S&P solution evaluation effort	To determine the extent to which one or more BD-S&P solutions meet BD-S&P objectives and address stakeholder concerns, or to determine the quality or completeness of BD-S&P.
	6.3.2.3	Monitor, assess and control the BD-S&P solution evaluation activities	
	6.3.2.4	Determine evaluation criteria	
	6.3.2.5	Determine evaluation methods and integrate with evaluation objectives and criteria	
	6.3.2.6	Establish measurement techniques, methods and tools	
	6.3.2.7	Review evaluation-related information	
	6.3.2.8	Analyse BD-S&P solution attributes and assess stakeholder value	
	6.3.2.9	Characterize BD-S&P solution(s) based on assessment results	
	6.3.2.10	Formulate findings and recommendations	
	6.3.2.11	Capture and communicate evaluation results	

7 Guidance on security and privacy operations for big data

7.1 General

This section provides guidance on security and privacy operations in relation to the roles, activities and functional components defined in the BDRA.

Figure 3 describes the relationships between organizations and the BDRA:

- an organization is a part of an ecosystem which follows the BDRA. The BDRA consists of roles and sub-roles, activities and functional components;
- an organization implements operations that are related to roles, activities and functional components. For instance, an organization can be in charge of the big data application provider role; and
- an organization implements operations focusing on security and privacy. They are applied to protect assets in the BDRA against vulnerabilities. Some assets may be specific to an organization, e.g. commercially sensitive information, while others may be shared within the ecosystems, e.g. datasets.

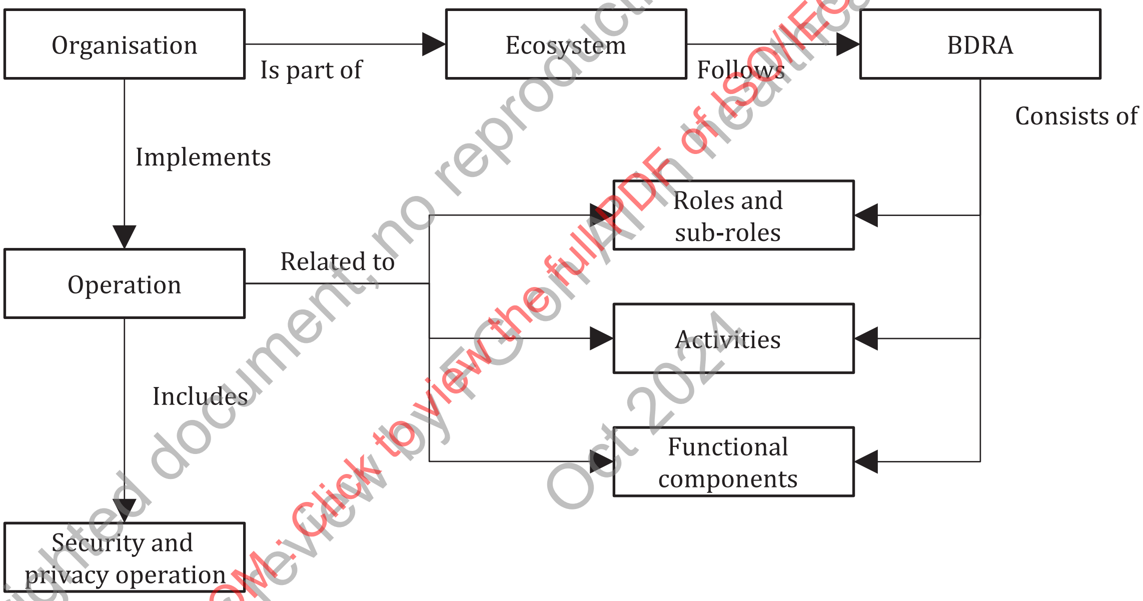

Figure 3 — Relationship between organizations and BDRA

As shown in Figure 4, this clause focuses on two types of security and privacy operations:

- organization operations; and
- ecosystem collaboration operations.

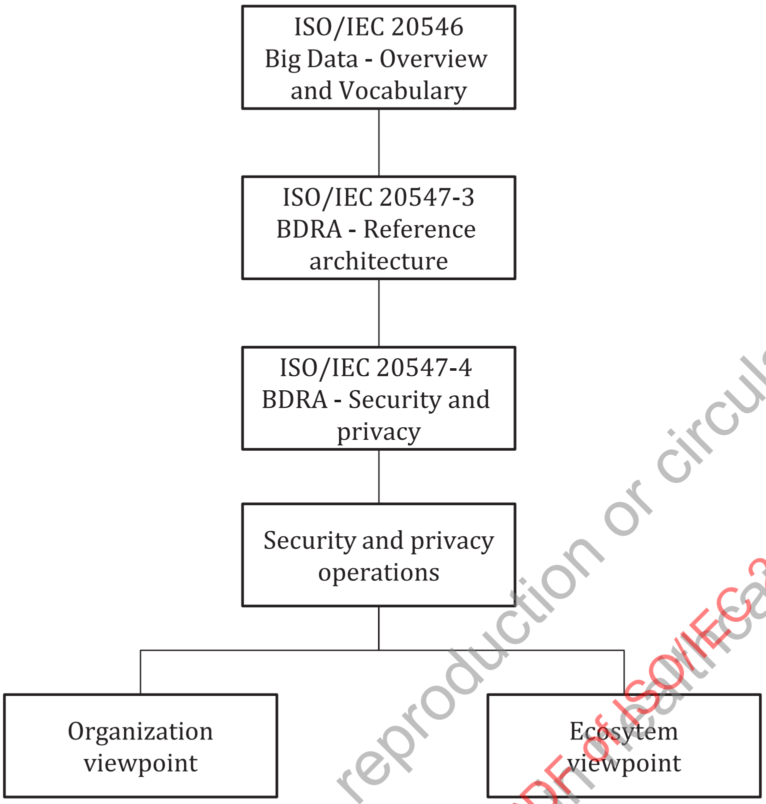
ISO/IEC 20546
Big Data - Overview and Vocabulary
ISO/IEC 20547-3
BDRA - Reference architecture
ISO/IEC 20547-4
BDRA - Security and privacy
Security and privacy operations
Organization viewpoint
Ecosytem viewpoint

Figure 4 — Two viewpoints on security and privacy operations

7.2 Guidance at organization level

7.2.1 General

Figure 5 shows the various standards that can be used to guide organizations in their big data security and privacy operations. There are four important phases:

- requirements phase;
- risk analysis phase;
- control design phase; and
- lifecycle engineering phase.

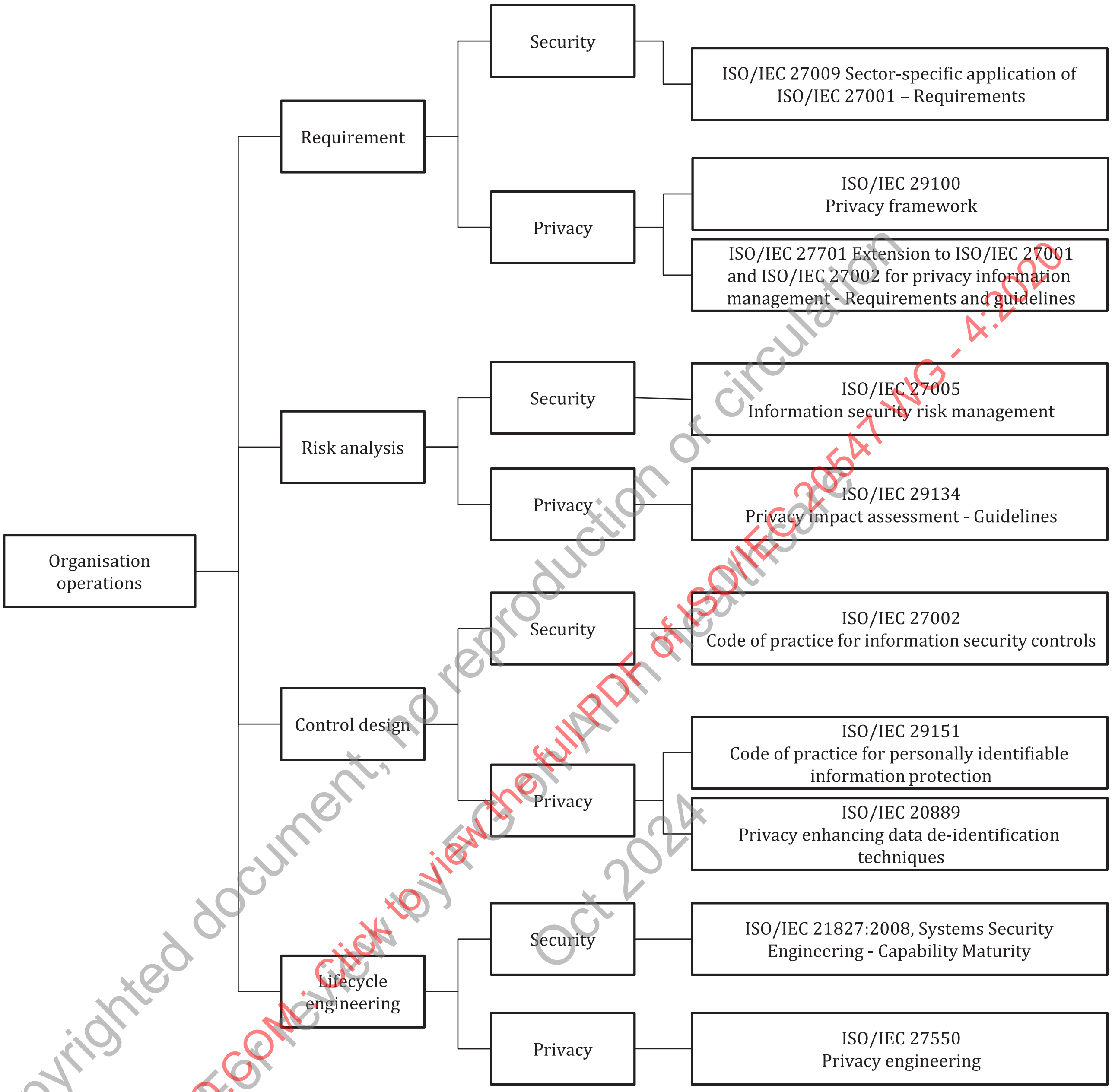
Organisation operations
Requirement
Risk analysis
Control design
Lifecycle engineering
Security
Privacy
Security
Privacy
Security
Privacy
Security
Privacy
ISO/IEC 27009 Sector-specific application of ISO/IEC 27001 – Requirements
ISO/IEC 29100 Privacy framework
ISO/IEC 27701 Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines
ISO/IEC 27005 Information security risk management
ISO/IEC 29134 Privacy impact assessment - Guidelines
ISO/IEC 27002 Code of practice for information security controls
ISO/IEC 29151 Code of practice for personally identifiable information protection
ISO/IEC 20889 Privacy enhancing data de-identification techniques
ISO/IEC 21827:2008, Systems Security Engineering - Capability Maturity
ISO/IEC 27550 Privacy engineering

Figure 5 — Standards for security and privacy operations

7.2.2 Standard guidance on requirements

Big data security and privacy operations dealing with requirements follow the following standards:

- security requirements of big data information systems as described in ISO/IEC 27001;
- sector-specific security requirements of big data information systems as described in ISO/IEC 27009;
- privacy requirements of big data systems resulting from the use of privacy principles as described in ISO/IEC 29100;
- privacy requirements of big data information systems as described in ISO/IEC 27701.

7.2.3 Standard guidance on risk management

Big data security and privacy operations dealing with risk analysis follow the following standards:

- information security risk management as described in ISO/IEC 27005;
- privacy impact assessment guidelines as described in ISO/IEC 29134.

7.2.4 Standard guidance on controls

Big data security and privacy operations dealing with risk analysis follow the following standards:

- code of practice for information security controls as described in ISO/IEC 27002;
- code of practice for PII protection as described in ISO/IEC 29151;
- privacy enhancing data de-identification techniques as described in ISO/IEC 20889.

7.2.5 Standard guidance on lifecycle operations

Big data security and privacy operations dealing with lifecycle engineering follow the following standards:

- security engineering as described in ISO/IEC 21827;
- privacy engineering as described in ISO/IEC TR 27550.

7.3 Guidance at ecosystem level

7.3.1 General

An organization can be in charge of:

- BDRA roles, e.g. big data provider, big data application provider, big data consumer;
- BDRA sub-roles, e.g. big data collection provider, big data analytics provider, which are sub-roles of big data application provider role;
- supplying BDRA functional components. They can be:
  - components in one of the BDRA architecture layer, e.g. a streaming capability in the processing layer, or a visualization component in the platform layer; or
  - components in the multi-layer functions part of the BDRA architecture, e.g. an authentication capability; and
- a combination of roles, sub-roles and supplying functional components.

Security and privacy can involve global assets shared by organizations within a big data ecosystem. In that case, their security and privacy operations should be coordinated as shown in Figure 6:

- each organization carries out its own security and privacy operations;
- overall coordination of each organizations' security and privacy operations ensures consistency.

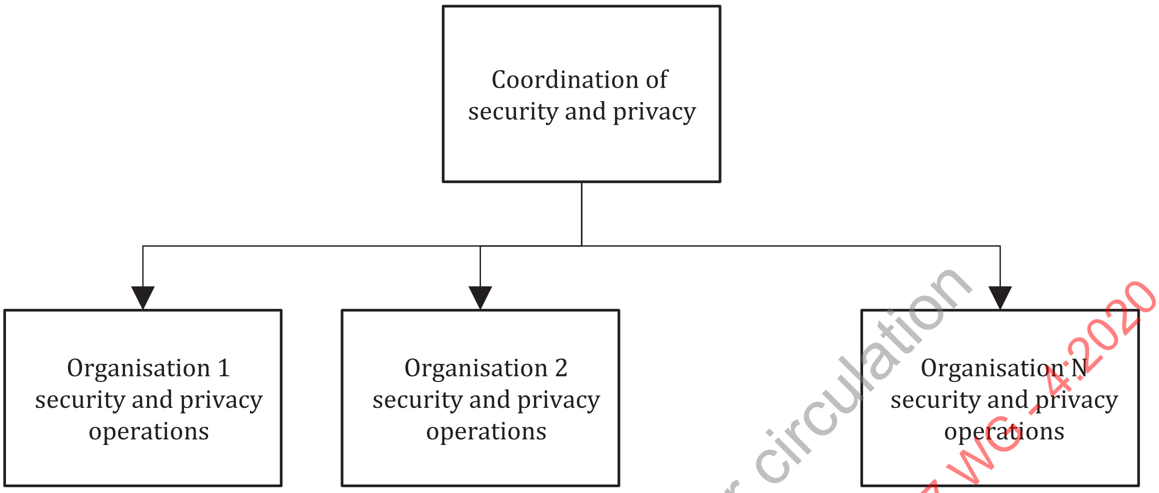
Coordination of security and privacy
Organisation 1 security and privacy operations
Organisation 2 security and privacy operations
Organisation N security and privacy operations

Figure 6 — Coordination of security and privacy operations

Coordination can take different forms, e.g. a public authority, a dedicated organization, an alliance. Here are examples of security and privacy management coordination:

- organizations involved in traffic big data to allow for smart traffic analytics apply security and privacy operations that can be coordinated by a city authority;
- organizations involved in healthcare big data to allow for clinical analytics apply security and privacy operations that can be coordinated by national health authority;
- organizations involved in insurance big data to allow for insurance risk analysis apply security and privacy operations that can be coordinated by an ad-hoc working group.

This sub-clause provides guidance on the coordination of the following security and privacy operations in big data ecosystems:

- data sharing, which belongs to the agreement category (ISO/IEC/IEEE 15288);
- security and risk analysis, which belongs to the technical management category (ISO/IEC/IEE 15288);
- lifecycle management, which belongs to the technical category (ISO/IEC/IEEE 15288).

7.3.2 Guidance on data processing chain

Coordination is needed when a data processing chain is in operation. For instance, an IoT system operator can collect data that is provided as a dataset to a service provider which in turn combines it with other sources of data and provides it to a data consumer. As shown in Figure 7:

- each organization carries out its data sharing operations;
- overall coordination of each organization's data sharing operations ensures the security and privacy of the data processing chain.

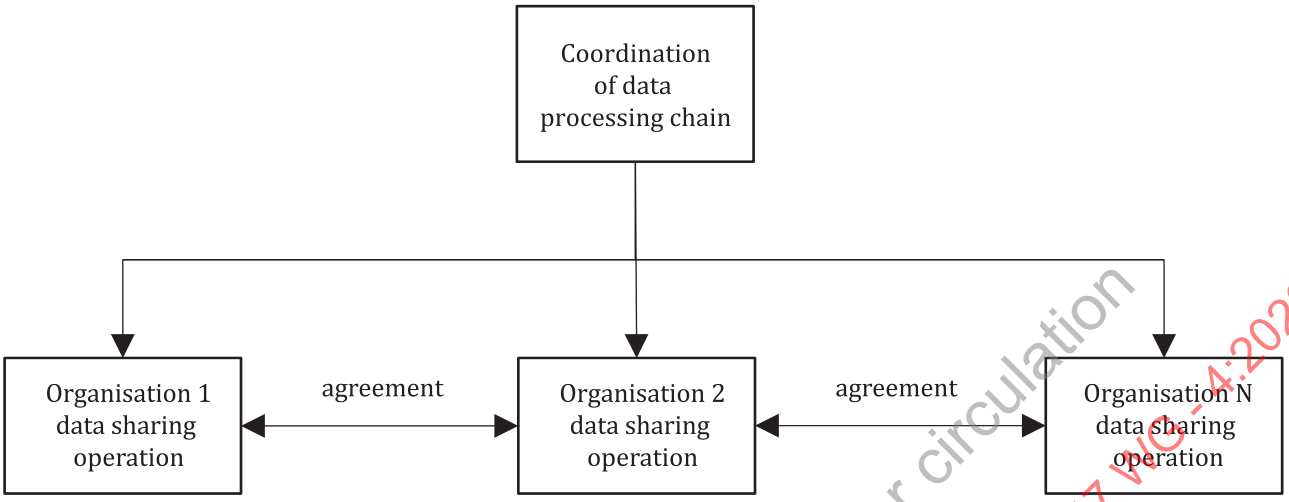
Coordination of data processing chain
Organisation 1 data sharing operation
agreement
Organisation 2 data sharing operation
agreement
Organisation N data sharing operation

Figure 7 — Coordination of data processing chain

The following guidance is provided:

- at the ecosystem level:
  - identify the data processing chain operational requirements such as velocity, veracity, scalability, provenance;
  - identify the security and privacy protection requirements of the data processing chain, such as data confidentiality, integrity, availability, unlinkability, transparency, intervenability;
  - identify specific requirements associated with BDRA roles, sub-roles, activities and functional components; and
  - establish security and privacy coordination schemes in the ecosystem, including measures for compliance, assurance and audit of practice;
- at the organization level:
  - identify the specific organization operational requirements such as velocity, veracity, scalability, provenance;
  - identify the specific organization security and privacy protection requirements on data confidentiality, integrity, availability, unlinkability, transparency, intervenability; and
  - establish data sharing operations in accordance with the ecosystem coordination scheme.

7.3.3 Guidance on risk management

Coordination is needed for security and privacy risk management. For instance, if the data collected by an IoT system operator and provided as a dataset to a service provider is compromised, then the operations of the service provider are compromised. As shown in Figure 8:

- each organization carries out its security and privacy risk management operations;
- overall coordination of security and privacy risk management ensures a common understanding of the risks at the ecosystem level.

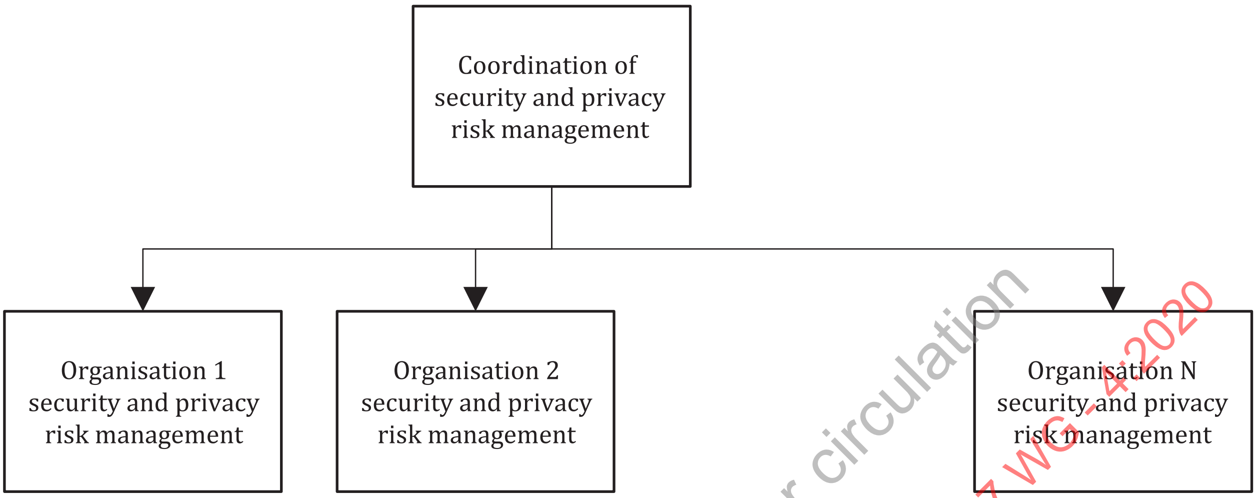
Coordination of security and privacy risk management
Organisation 1 security and privacy risk management
Organisation 2 security and privacy risk management
Organisation N security and privacy risk management

Figure 8 — Coordination of security and privacy risk management

The following guidance is provided:

- at the ecosystem level:
  - identify the vulnerabilities and threats of the ecosystem that need coordination. It is advised that organizations in the ecosystem provide descriptions based on common classifications. Annex A provides, as examples, the STRIDE and LINDDUN classification;
  - identify the risks and breaches of the ecosystem;
  - identify the controls to treat the risks of the ecosystem;
  - identify specific security and privacy risk management requirements associated with BDRA roles, sub-roles, activities and functional components; and
  - establish security and privacy risk management coordination schemes in the ecosystem, including measures for monitoring risks and for compliance, assurance and audits of practice;
- at the organization level:
  - identify the vulnerabilities and threats of the system which the organization is responsible for in the ecosystem;
  - identify the risks and breaches of the system;
  - identify the controls to treat the risks of the system;
  - establish security and risk management operations in accordance with the ecosystem coordination scheme.

7.3.4 Guidance on lifecycle operations

Coordination is needed on the security and privacy lifecycle of big data. For instance,

- organizations can agree on the use of similar controls, for example:
  - an agreed level of protection for data at rest;
  - an agreed level of integrity and authentication for data in motion;
  - an agreed level of availability for data processing;

  - an agreed level of unlinkability for data provenance;
- organizations can agree on coordination for incident management, for example:
  - an agreed level of incident preparedness;
  - a common alert mechanism on security breaches (e.g. tampering detection) or on privacy breaches (e.g.re-identification detection).

As shown in Figure 9:

- each organization carries out its security and privacy lifecycle operations;
- overall coordination of security and privacy lifecycle ensures consistent treatment of the assets to protect.

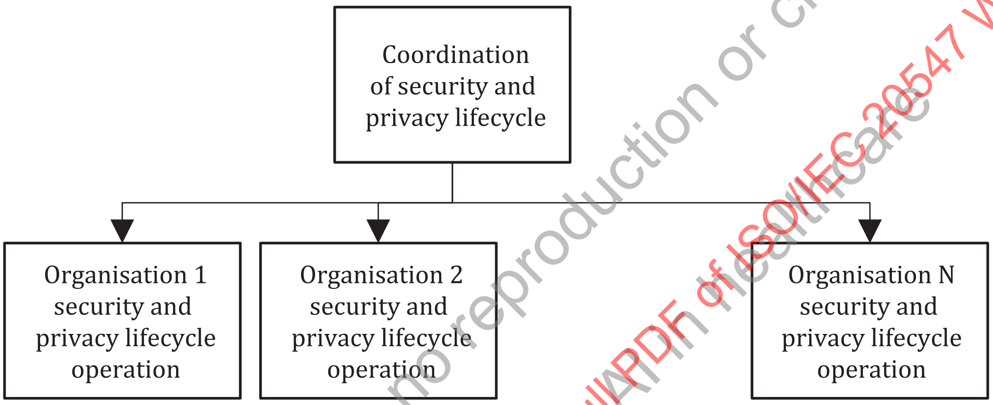
Coordination of security and privacy lifecycle
Organisation 1 security and privacy lifecycle operation
Organisation 2 security and privacy lifecycle operation
Organisation N security and privacy lifecycle operation

Figure 9 — Coordination of security and privacy lifecycle

The following guidance is provided:

- at the ecosystem level:
  - identify the operations in the ecosystem lifecycle where coordination is needed (assurance, compliance verification, incident management, audit);
  - identify the controls that are implemented in the ecosystem further to the risk analysis coordination. It is advised that organizations in the ecosystem provide control descriptions based on common classifications. Annex B provides, as example, the categorization used in ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27701, ISO/IEC 29151;
  - establish control coordination schemes in the ecosystem, including measures for compliance, assurance and audits of controls;
- at the organization level:
  - identify the operations in the system lifecycle where security and privacy concerns need to be integrated;
  - identify the controls that are implemented in the system further to the risk analysis;
  - establish the lifecycle operations in accordance with the ecosystem coordination scheme.

Annex C provides, as examples, the ecosystem and resulting coordination of security and privacy operations.

8 Security and privacy functional components

8.1 Overview

Clause 7 describes the BDRA-S&P in terms of the common set of functional components. A functional component is a functional element of the BDRA-S&P which is used to perform an activity or some part of an activity and which has an implementation artifact in a concrete realization of the architecture.

Security and privacy controls provided in existing standards can be utilized to realize the security and privacy functional components with additional consideration of the security and privacy objectives in the context of big data. Annex B lists the security and privacy control categories specified in ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27701, ISO/IEC 29151.

8.2 Functional components for both security and privacy

The security control categories specified in ISO/IEC 27002 are used in this document as functional components for both security and privacy, which are as follows.

a) **Information security policies** to provide management direction and support for information security in accordance with business requirements and taking into consideration compliance with relevant laws and regulations.

b) **Organization of information security** to establish a management framework to initiate and control the implementation and operation of information security within the organization.

c) **Human resource security** to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered prior to employment, to ensure that employees and contractors are aware of and fulfil their information security responsibilities during employment, to protect the organization’s interests as part of the process of changing or terminating employment when termination and change of employment.

d) **Asset management** to identify organizational assets and define appropriate protection responsibilities, to ensure that information receives an appropriate level of protection in accordance with its importance to the organization by information classification, to prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

e) **Access control** to limit access to information and information processing facilities, to ensure authorized user access and to prevent unauthorized access to systems and services, to make users accountable for safeguarding their authentication information, to prevent unauthorized access to systems and applications.

f) **Cryptography** to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

g) **Physical and environmental security** to prevent unauthorized physical access, damage and interference to the organization’s information and information processing facilities, to prevent loss, damage, theft or compromise of assets and interruption to the organization’s operations.

h) **Operation security** to ensure correct and secure operations of information processing facilities, to ensure that information and information processing facilities are protected against malware, to protect against loss of data by backup, to record events and generate evidence by logging and monitoring, to ensure the integrity of operational systems by control of operational software, to prevent exploitation of technical vulnerabilities, to minimize the impact of audit activities on operational systems.

i) **Communication security** to ensure the protection of information in networks and its supporting information processing facilities, to maintain the security of information transferred within an organization and with any external entity.

j) **System acquisition, development and maintenance** to ensure that information security is an integral part of information systems across the entire lifecycle (also including the requirements for information systems which provide services over public networks), to ensure that information security is designed and implemented within the development lifecycle of information systems, to ensure the protection of data used for testing.

k) **Suppliers relationships** to ensure the protection of the organization's assets that is accessible by suppliers, to maintain an agreed level of information security and service delivery in line with supplier agreements

l) **Information security incident management** to ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

m) **Information security aspects of business continuity management** that should be embedded in the organization's business continuity management systems, to ensure the availability of information processing facilities by redundancies.

n) **Compliance** with legal, statutory, regulatory, or contractual obligations related to information security and of any security requirements is presupposed, to ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

Annex D provides, as examples, the security and privacy controls for big data application provider (BDAP) and big data provider (BDP).

8.3 Functional components for privacy

The privacy control categories for PII controllers and PII processors specified in ISO/IEC 27701 are used in this document as functional components for privacy, which are as follows.

a) **Conditions for collection and processing** to determine and document that processing is lawful, with legal basis as per applicable jurisdictions and with clearly defined and legitimate purposes.

b) **Rights of PII principals** to ensure that PII principals are provided with appropriate information about the processing of their PII and to meet any other applicable obligations to PII principals related to the processing of their PII.

c) **Privacy-by-design and by-default** for PII controllers to ensure that processes and systems are designed such that the collection and processing of PII (including use, disclosure, retention, transmission and disposal) are limited to what is necessary for the identified purpose.

d) **PII sharing, transfer and disclosure** to determine whether and document when PII is shared, transferred to other jurisdictions or third parties and/or disclosed in accordance with applicable obligations.

Other dimensions to view functional components for privacy are as follows.

a) **Privacy policy enforcement**

An organization as PII controller should define their privacy policy, how they protect personal data inside the organization, in the product development process, etc. The privacy policy can contain the classification of personal data, privacy risk assessment, data sharing policy and required protection mechanisms necessary in the data life cycle. The protection mechanisms include encryption, de-identification, access control policy, etc. It is recommended to use IT tools and extend the existing IT security systems to enforce privacy policy so that personal data is protected according to the policy and violation of the policy can be detected.

b) **Personal data detection and inventory**

This component can detect personal data in data storage or before data transfer and collection. Detection of personal data in unstructured data such as in a document, audio or video files relies on rule-based and machine learning methods. The source of personal data needs to be recorded. The data should be classified and tagged based on their sensitivity. Additionally, data belonging to the same data subjects need to be inventoried, that can facilitate the management of personal data. In the case that a data subject requires to delete his/her personal data, related data can be easily found.

c) **De-identification**

This component can modify personal data so that the identities of data subjects are obscured. It reduces the sensitivity of personal data in the sense that it is hard to link to the data subject or it reduces information expose about the data subject. It also reserves the utility to a certain extent to meet business requirements. The technologies commonly used for the de-identification of structured datasets are described in ISO/IEC 20889:2018. The selection of the technologies depends on the privacy risks of given scenarios and the defined privacy policy of an organization. A trade-off between privacy protection and data utility needs to be made. De-identification technologies should be applied as early as possible during the data life cycle to reduce privacy risks in further processing steps. The technologies should support large scale applications in the context of big data.

d) **Privacy risk assessment**

This component can give a qualitative assessment based on the sensitivity of the data. For instance, an organization can divide privacy risks into 5 levels and require different protection strategies. Alternatively, quantitative assessment can be given based on the empirical evaluation. The evaluation metrics can be defined based on potential privacy attacks on data. Since data of a data subject can be collected from different applications and stored in different big data subsystems, privacy risks linking different data sources need to be taken into account and evaluated. Some de-identification techniques such as differential privacy, k-anonymity, l-diversity, etc., provide metrics to quantify privacy risk. Privacy risks should be continuously monitored during the data life cycle, especially when data is changed or made used in other contexts.

e) **Privacy-preserving computation**

This component can protect the privacy of data in use. In the big data market, the data provider can want to monetize the data without revealing data to the data consumer. Alternatively, different PII controllers want to combine their data to train a machine learning model. Technologies such as secure set intersection, secure multiparty computation, homomorphic encryption, secure enclaves can be used to support privacy-preserving computation.

f) **Access control and monitoring**

This component provides access control management and monitors access to personal data. It can detect invalid access and avoid data leakage.

g) **Data subject right protection**

The component enables functions, which is necessary to ensure data subject rights. For instance, the consent management model can record when a data subject give/withdraw their consent of data collection and usage of an applications. It can securely remove or anonymize data according to requests of the data subject or after data retention time. In a big data system, data of the same data subject can be located in different places of different applications. Data inventory can very help to locate personal data.

8.4 Multi-layer functions for security and privacy

The following multi-layer functions for both security and privacy are specified in ISO/IEC 20547-3 (see ISO/IEC 20547-3:2020, Figure 12 and 10.2.6.3):

— audit framework;

— authentication framework;

- authorization framework;
- anonymization framework.

As shown in Table 4, these frameworks can be supported by the functional components in 8.2 and 8.3.

Table 4 — Multi-layer functions and their supporting functional components for security and privacy

Multi-layer functions	Supporting functional components
Audit framework	8.2 n)
Authentication framework	8.2 e), 8.3 j)
Authorization framework	8.2 e), 8.3 b), 8.3 d), 8.3 j), 8.3 k)
Anonymization framework	8.3 g)

Annex A
(informative)

Examples of security and privacy threat classification

Table A.1 and Table A.2 list categories of security and privacy threats. Security threats follow the STRIDE categorization. Privacy threats follow the LINDDUN categorization.

Table A.1 — STRIDE security threats categories

Threat	Property	Property description
Spoofing	Authentication	The identity of users is established (or you are willing to accept anonymous users).
Tampering	Integrity	Data and system resources are only changed in appropriate ways by appropriate people.
Repudiation	Nonrepudiation	Users cannot perform an action and later deny performing it.
Information disclosure	Confidentiality	Data is only available to the people intended to access it.
Denial of service	Availability	Systems are ready when needed and perform acceptably.
Elevation of privilege	Authorization	Users are explicitly allowed or denied access to resources.

Table A.2 — LINDDUN privacy threats categories

Threat	Property		Property description
Linkability	Hard privacy	Unlinkability	Hiding the link between two or more actions, identities and pieces of information.
Identifiability		Anonymity	Hiding the link between an identity and an action or a piece of information
Non-repudiation		Plausible deniability	Ability to deny having performed an action that other parties can neither confirm nor contradict
Detectability		Undetectability and unobservability	Hiding the user's activities
Disclosure of information	Security	Confidentiality	Hiding the data content or controlled release of data content
Unawareness	Soft Privacy	Content awareness	User's consciousness regarding his own data
Non-compliance		Policy and consent compliance	PII controller to inform the data subject to the system's privacy policy, or allow the data subject to specify consents in compliance with legislation

Annex B
(informative)

Examples of security and privacy control classification

Table B.1 lists control categories as proposed by ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27701 and ISO/IEC 29151.

Table B.1 — Control categories

Category	Sub-categories
Information security policies	Management direction
Organization of information security	Internal organization Mobile devices and teleworking
Human resource security	Prior to employment During employment Termination and change of employment
Asset management	Responsibility for assets Information classification
Access control	Business requirements of access control User access management User responsibilities System and application access control Media handling
Cryptography	Cryptographic controls
Physical and environmental security	Secure areas Equipment
Operation security	Operational procedures and responsibilities Protection from malware Backup Logging and monitoring Control of operational software Technical vulnerability management Information systems audit considerations
Communication security	Network security management Information transfer
System acquisition, development and maintenance	Security requirements of information system Security in development and support processes Test data
Suppliers relationships	Information security in supplier relationships Supplier service delivery management

Table B.1 *(continued)*

Category	Sub-categories
Information security incident management	Management of information security incidents and improvements
Information security aspects of business continuity management	Information security continuity Redundancies
Compliance	Compliance with legal and contractual requirements Information security reviews

Table B.2 and Table B.3 list further privacy controls as proposed by ISO/IEC 27701, depending on whether the organization is a PII controller or a PII processor.

Table B.2 — Privacy controls for PII controllers

Category	Measures for PII controllers
Conditions for collection and processing	Identify and document purpose
	Identify lawful basis
	Determine when and how consent is to be obtained
	Obtain and record consent
	Privacy impact assessment
	Contracts with PII processors
	Records related to processing PII
Rights of PII principals	Determining PII principals rights and enabling exercise
	Determining information for PII principals
	Providing information for PII principals
	Provide mechanism to modify of withdraw consent
	Provide mechanism to object to processing
	Sharing the exercising of PII principle
	Correction or erasure
	Providing copy of PII processed
	Request management
	Automated decision making
Privacy-by-design and by-default	Limit collection
	Limit processing
	Define and document PII minimization and de-identification objectives
	Comply with data minimization and de-identification use
	PII de-identification and deletion
	Temporary files
	Retention
	Disposal
	Collection procedures
	PII transmission controls
PII sharing, transfer and disclosure	Identify basis for PII transfer
	Countries and organizations to which PII may be transferred
	Records of transfer of PII
	Records of PII disclosure to third parties
	Joint controller

Table B.3 — Privacy controls for PII processors

Category	Measures for PII Processors
Conditions for collection and processing	Cooperation agreement
	Organization’s purposes
	Marketing and advertising use
	Infringing instruction
	PII controller obligations
	Records related to processing PII
Rights of PII principals	Obligations to PII principals
	Limit processing
Privacy-by-design and by-default	Temporary files
	Return transfer or disposal of PII
	PII transmission controls
PII sharing, transfer and disclosure	Basis for transfer of PII
	Countries and organizations to which PII may be transferred
	Records of PII disclosure to third parties
	Notification of PII disclosure requests
	Legally binding PII disclosures
	Disclosure of subcontractors used to process PII
	Engagement of a subcontractor to process PII
	Change of subcontractor to process PII

Annex C
(informative)

Examples of ecosystem and resulting coordination of security and privacy operations

C.1 Mapping organizations of the ecosystem to BDRA

This example is adapted from the AutoMat automotive big data research project. The purpose of the example is to show concrete examples of how the ecosystem is coordinated. The ecosystem involves the following organizations (see Figure C.1):

- automotive manufacturers play the big data provider BDRA role, as well as the big data collection provider and big data preparation provider BDRA sub-roles. They install with the consent of vehicle owners a data collecting system, collect data and prepare them into an interoperable format (common vehicle information model);
- storage providers play the big data infrastructure provider BDRA sub-role. They manage data at rest. Data collected are stored and managed separately in vehicle owner accounts;
- marketplaces play the big data platform provider and big data processing provider BDRA sub-roles. The collected data from the storage providers and transform them into datasets that can be used by services providers; and
- service providers play the big data analytics provider, big data visualization provider, big data access provider BDRA sub-roles and the big data consumer BDRA role.

The following can be observed:

- the mapping between roles and organizations is not one-to-one;
- the storage provider customers are vehicle owners who directly control the use of data; and
- the marketplace builds on the fly datasets requested by service providers.

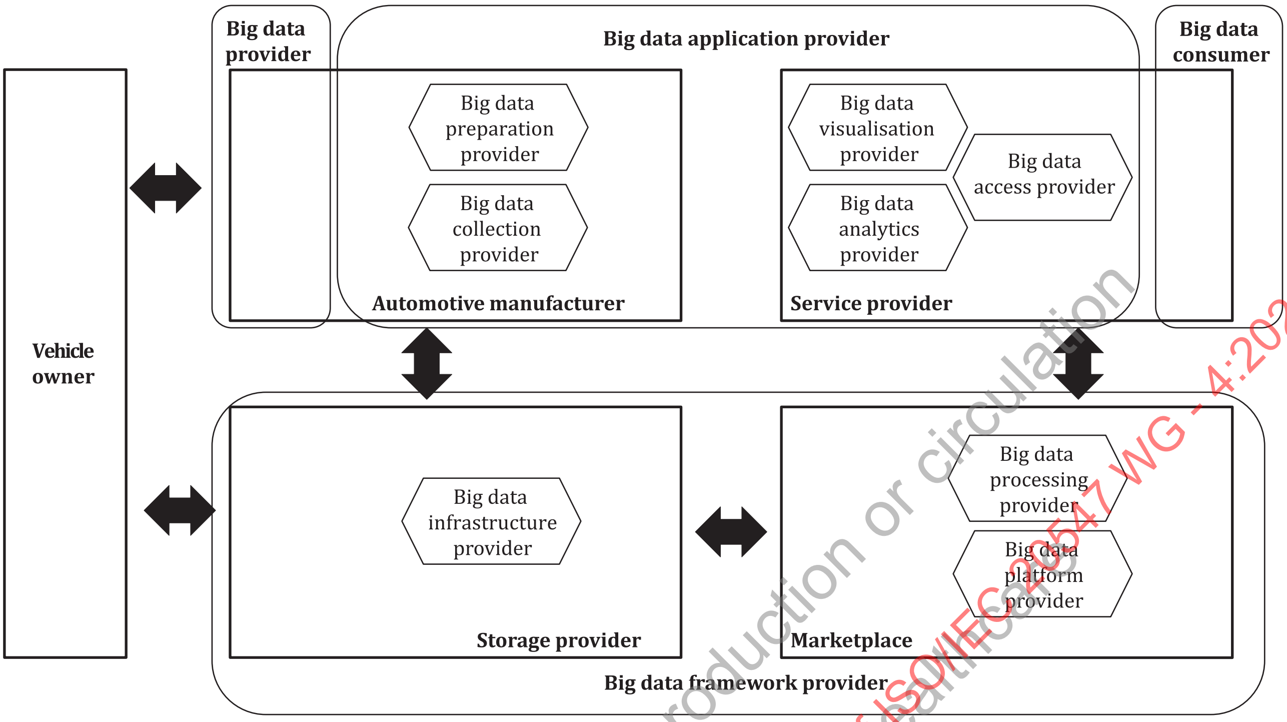
Big data provider
Big data application provider
Big data consumer
Big data preparation provider
Big data collection provider
Automotive manufacturer
Big data visualisation provider
Big data access provider
Big data analytics provider
Service provider
Vehicle owner
Big data infrastructure provider
Storage provider
Big data processing provider
Big data platform provider
Marketplace
Big data framework provider

Figure C.1 — Example of ecosystem following BDRA

C.2 Ecosystem coordination

The ecosystem follows the personal data ecosystem approach. While automotive manufacturers are part of the ecosystem as they play the role of big data provider and the sub-roles of big data collection provider and big data preparation provider, they are not involved in the exchange of data with service providers. This is managed by the marketplace which serves as the broker between vehicle owners and service providers. Figure C.2 shows the resulting two features of the ecosystem:

- data is stored according to vehicle accounts;
- an interoperable description is made available to the market place (called common vehicle information model or CVIM).

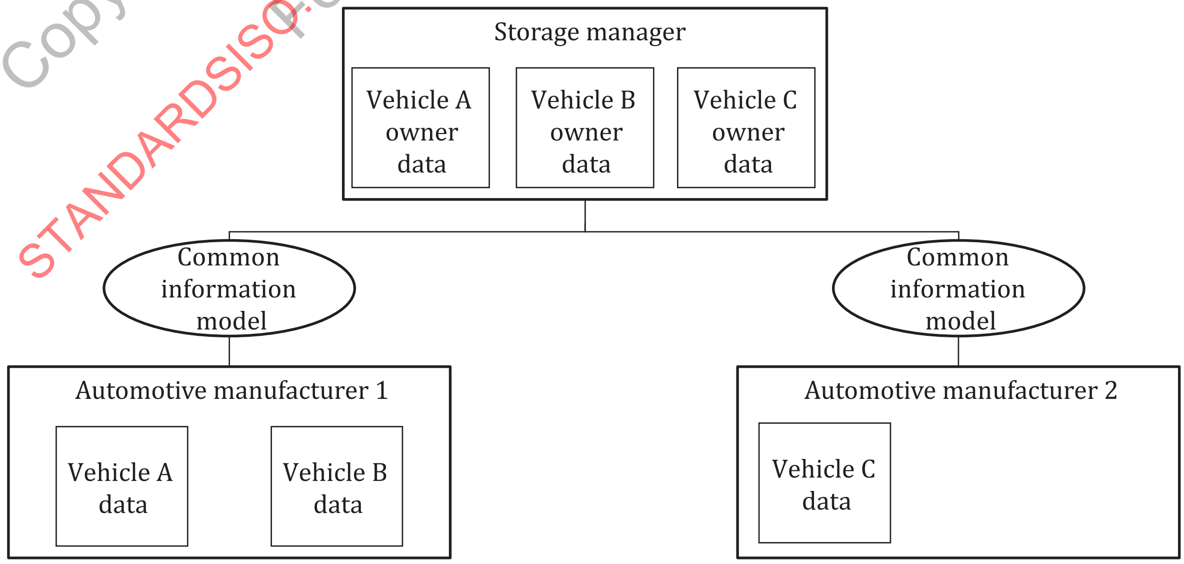

Figure C.2 — AutoMat personal data ecosystem