

---

---

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

**Part 4:  
Security and privacy**

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

**iTeh STANDARD PREVIEW**  
*Partie 4: Sécurité et confidentialité*  
**(standards.iteh.ai)**

ISO/IEC 20547-4:2020

<https://standards.iteh.ai/catalog/standards/sist/22cc47cd-9d99-4e5a-ad90-062792041b4c/iso-iec-20547-4-2020>



**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

ISO/IEC 20547-4:2020

<https://standards.iteh.ai/catalog/standards/sist/22cc47cd-9d99-4e5a-ad90-062792041b4c/iso-iec-20547-4-2020>



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
CP 401 • Ch. de Blandonnet 8  
CH-1214 Vernier; Geneva  
Phone: +41 22 749 01 11  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

	Page
<b>Foreword</b> .....	<b>v</b>
<b>Introduction</b> .....	<b>vi</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Symbols and abbreviated terms</b> .....	<b>1</b>
<b>5 Overview</b> .....	<b>2</b>
5.1 Big data security and privacy concerns.....	2
5.2 Security and privacy objectives.....	4
<b>6 Security and privacy aspects of BDRA user view</b> .....	<b>6</b>
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
<b>7 Guidance on security and privacy operations for big data</b> .....	<b>29</b>
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
<b>8 Security and privacy functional components</b> .....	<b>37</b>
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

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

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[ISO/IEC 20547-4:2020](https://standards.iteh.ai/catalog/standards/sist/22cc47cd-9d99-4e5a-ad90-062792041b4c/iso-iec-20547-4-2020)

<https://standards.iteh.ai/catalog/standards/sist/22cc47cd-9d99-4e5a-ad90-062792041b4c/iso-iec-20547-4-2020>

## 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](http://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](http://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](http://www.iso.org/iso/foreword.html) ([standards.iteh.ai](http://standards.iteh.ai)).

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](http://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.

## iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/IEC 20547-4:2020](https://standards.iteh.ai/catalog/standards/sist/22cc47cd-9d99-4e5a-ad90-062792041b4c/iso-iec-20547-4-2020)

<https://standards.iteh.ai/catalog/standards/sist/22cc47cd-9d99-4e5a-ad90-062792041b4c/iso-iec-20547-4-2020>

# 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*  
<https://standards.iteh.ai/catalog/standards/sist/22cc47cd-9d99-4e3a-ad90-062792041b4c/iso-iec-20547-4-2020>

### 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.