International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1750

(09/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Data security – Big Data Security

Guidelines on security of big data as a service for big data service providers

Recommendation ITU-T X.1750

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	**X.1750–X.1759**
5G SECURITY	X.1800–X.1819

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1750

Guidelines on security of big data as a service for big data service providers

Summary

Big data as a service (BDaaS) is a cloud service category that provides cloud service customers with capabilities to collect, store, analyse, visualize and manage big data, as specified in Recommendation ITU-T Y.3600. With remarkable growth of data volumes and rapid development of big data business, big data infrastructure has become the central facility to provide BDaaS. Consequently, significant security issues arise for BDaaS. For example, open source big data software design sometimes fails to take security into consideration from the beginning. New technologies introduced by big data analytics can also result in failure of traditional security protection measures. Recommendation ITU-T X.1750 analyses security challenges BDaaS faces, identifies security roles and responsibilities for provision of BDaaS, as well as a security framework for a big data infrastructure. It also specifies security protection measures that should be satisfied for services and components related to BDaaS.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1750	2020-09-03	17	11.1002/1000/14266

Keywords

Big data as a service, security guidelines, security measures.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1750

Guidelines on security of big data as a service for big data service providers

1 Scope

This Recommendation analyses security challenges faced by big data as a service (BDaaS) and provides guidelines for big data service providers (BDSPs) to secure BDaaS. It identifies security roles and responsibilities of BDaaS components and specifies a security framework for a big data infrastructure, including platforms, applications, analytics, interfaces and the BDaaS ecosystem. This Recommendation also specifies security protection measures that should be taken for activities or components related to BDaaS.

This Recommendation is a high-level description of security requirements for BDaaS implementation that focuses on BDaaS. BDaaS involves big data infrastructure providers (BDIPs) and big data application providers (BDAPs). Guidelines for BDIPs and BDAPs, as well as detailed guidance on BDaaS implementation lie outside the scope of this Recommendation.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.

[ITU-T X.1631] Recommendation ITU-T X.1631 (2015), *Information technology – Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services*.

[ITU-T X.1641] Recommendation ITU-T X.1641 (2016), *Guidelines for cloud service customer data security*.

[ITU-T Y.3600] Recommendation ITU-T Y.3600 (2015), *Big data – Cloud computing based requirements and capabilities.*

[ISO/IEC 27000] ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[ISO/IEC 27036-3] ISO/IEC 27036-3:2013, *Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security*.

[ISO 28000] ISO 28000:2007, *Specification for security management systems for the supply chain.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 big data [ITU-T Y.3600]: A paradigm for enabling the collection, storage, management, analysis and visualization, potentially under real-time constraints, of extensive datasets with heterogeneous characteristics.

NOTE – Examples of datasets characteristics include high-volume, high-velocity, high-variety, etc.

3.1.2 big data as a service (BDaaS) [ITU-T Y.3600]: A cloud service category in which the capabilities provided to the cloud service customer are the ability to collect, store, analyse, visualize and manage data using big data.

3.1.3 big data provenance [b-ITU-T Y.3602]: Information that records the historical path of data according to the data lifecycle operations in a big data ecosystem.

3.1.4 cloud computing [b-ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

3.1.5 cloud service [b-ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.6 metadata [b-ITU-T M.3030]: Data that describes other data.

3.1.7 security challenge [ITU-T X.1601]: A security "difficulty" other than a direct security threat arising from the nature and operating environment of cloud services, including "indirect" threats.

3.1.8 threat [ISO/IEC 27000]: Potential cause of an unwanted incident, which can result in harm to a system or organization.

3.1.9 vulnerability [b-NIST SP 800-30]: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 data asset: An electronically recorded data resource, owned or controlled by an organization.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Programming Interface

ABAC Attribute-Based Access Control

BDaaS Big Data as a Service

BDAP Big Data Application Provider

BDIP Big Data Infrastructure Provider

BDSN Big Data Service partner

BDSP Big Data Service Provider

BDSU Big Data Service User

CSC Cloud Service Customer

DP Data Provider

IT Information Technology

PII Personally Identifiable Information

PKI Public Key Infrastructure

SAML Security Assertion Markup Language

SDK Software Development Kit

SSL Secure Socket Layer

TLS Transport Layer Security

USB Universal Serial Bus

5 Conventions

In this Recommendation:

The phrase "**is required to**" indicates a requirement that must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The phrase "**is recommended**" indicates a requirement that is recommended, but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The phrase "**is prohibited from**" indicates a requirement that must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The phrase "**can optionally**" indicates an optional requirement that is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator or service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Security threats and challenges to big data as a service

This clause describes security threats and challenges to BDaaS. Cloud computing-based BDaaS is specified in [ITU-T Y.3600]. Security challenges relevant to cloud computing environments as described in clause 8 of [ITU-T X.1601] should be taken into consideration for BDaaS. This Recommendation, then, describes security threats and challenges to specific capabilities and services of BDaaS, i.e., big data platform as a service and big data-related software as a service (recognizing that the BDaaS ecosystem includes data providers (DPs), BDAPs and BDIPs), including:

– vulnerabilities of big data infrastructure and failure of security measures;

– storage and audit problems incurred by unstructured data;

– security and regulation of interface between applications, platforms and service flow;

– other security concerns, e.g., trust, authentication and visualization.

Figure 6-1 shows an architecture of BDaaS security challenges.

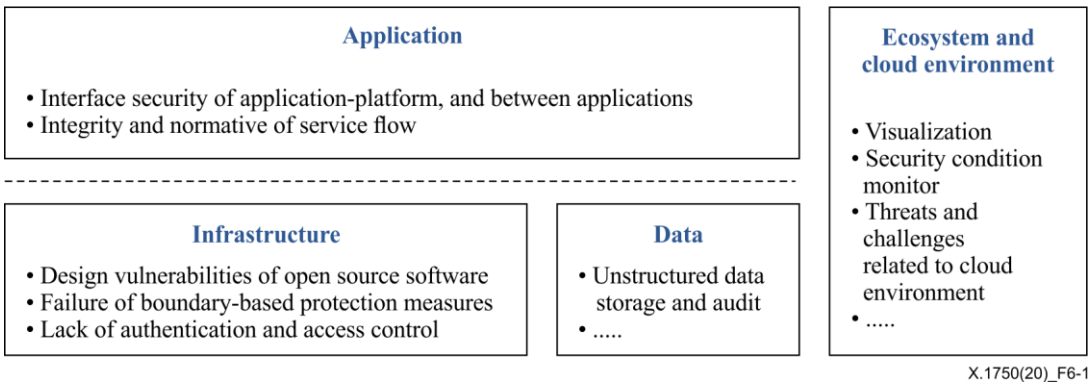

Figure 6-1 – Big data as a service security challenges

6.1 Security challenges to a big data infrastructure

Big data infrastructure may consist of various components sourced either commercially or through open source. The design of some of these components may fail to take security into consideration from the beginning, causing potential security risks, including:

– insecure source code and lack of security mechanisms in open source components;

– open and inter-domain platform characteristics that blur traditional security boundaries, causing failure of boundary-based protection measures; and

– lack of appropriate authentication and access control mechanisms for different roles may lead to abuse.

6.2 Security challenges to big data applications

A big data infrastructure integrates a variety of highly centralized applications with complicated service patterns. Security challenges to big data applications include:

– possible lack of security verification and transmission control for application programming interfaces (APIs), software development kits (SDKs) and interfaces between applications; and

– the need for execution of user applications to be traced, audited and located to guarantee business logic security.

6.3 Security challenges to data

Big data infrastructure and applications deal with massive quantities of data. Within a big data ecosystem, data types include structured, semi-structured and unstructured data. Structured data are often stored in databases that may be organized according to different models, e.g., relational, document, key-value and graph models. Semi-structured data does not conform to the formal structure of data models, but contains tags or markers to identify data. Unstructured data do not have a pre-defined data model and are not organized in any established manner. Different formats, e.g., text, spreadsheet, video, audio, image and map, can exist within all data types (see [ITU-T Y.3600]). That data is used in storage, analysis, calculation and other data service phases. Security challenges to data include:

– requirement for security measures (including access controls) to ensure data confidentiality, while still supporting efficient data operation;

– audit of unstructured data;

– risk of leakage of personal privacy information if data is open or shared;

– the need to apply traditional security measures described in [ITU-T X.1601] to metadata, as it has the same characteristics as data published on a web;

Security challenges to big data provenance handling include: contaminated or maliciously manipulated records throughout the chain of provenance processing, unauthorized entities in provenance data processing or exchange, unauthentic codes of processing for the data provenance, as well as security challenges to provenance data.

6.4 Security challenges to big data as a service ecosystem

According to [ITU-T Y.3600], a BDaaS ecosystem consists of roles and sub-roles played by different parties or components providing and consuming big data services. A BDaaS ecosystem is required to plan, design and implement security measures in construction, operation, auditing and other phases of service provenance. Security challenges to big data services include:

– the need for continuous monitoring of user action, network conditions, resource status, etc. to cope with changing threats;

– emerging new threat vectors and lack of potential protection mechanisms;
– inability to establish trust between various actors, including data owners and devices (to collect data);
– security of virtualization instantiation, e.g., security configuration and virtual image integrity;
– possibility of a complicated supply chain in a big data ecosystem – even a contractor who is not directly contracted with an organization may affect its business continuity.
– Risks related to the supply chain should be analysed and necessary measure should be taken, including security measures specified in [ISO/IEC 27000] [ISO 28000].

7 High-level concepts of big data as a service – security considerations and role of BDSPs

[ITU-T Y.3600] specifies an architecture of big data technology that is general, multi-level and made up of logical function components. Based on this architecture, big data service security capabilities cover both system security and data security.

From a system perspective, BDaaS security requirements cover capabilities of each related function module of 1) big data infrastructure; 2) big data application management; 3) interface security; and 4) operation and maintenance of big data platform security (the BDaaS ecosystem).

In particular, [ITU-T Y.3600] describes BDaaS as having two key components:

– BDIPs: can use the cloud services of cloud infrastructure capability types, such as compute as a service, data storage as a service, infrastructure as a service and network as a service to perform big data services like collection, processing and management.
– BDAPs: to perform data analysis, visualization and other big data applications.

From a data perspective, security requirements cover each activity in the process of big data service business development. Moreover, big data service capabilities also include security requirements for metadata and the data supply chain.

From the system view of BDaaS, [ITU-T Y.3600] identifies the system context including roles and activities, as well as data and service flows.

In terms of roles [ITU-T Y.3600], BDaaS services are offered by BDSPs that are responsible for ensuring security of BDaaS and reducing risks. It is recommended that BDSPs (BDIPs and BDAPs) consider both system security and data security to perform BDaaS activities.

8 Security measures of big data as a service

8.1 Security measures for a big data infrastructure

8.1.1 System asset security

8.1.1.1 General requirements

BDSPs shall:

– establish system asset security management strategies, clarify targets and principles of system asset security;
– establish construction and operation management policies and procedures of system assets, including planning, designing, purchasing, developing, operating, maintaining and scrapping;
– establish a system asset register mechanism, develop a system asset list, specify the security responsibility issue and related parties of system assets, and regularly maintain system asset information;

– establish and implement system asset classification and label procedures;
– perform regular audits and updates on information technology (IT) assets and security management policies.

8.1.1.2 Enhancement requirements

BDSPs should:

– identify the asset management controls available, such as those specified in [ITU-T X.1631], to perform component inventory and registration, auditing, and monitoring of system assets:
– establish asset risk evaluation procedures for the big data system, e.g., implementing a process to identify product or service components that are critical for maintaining functionality and therefore require increased attention and scrutiny;
– establish security assessment procedures for supply chain, such as those defined in [ISO/IEC 27036-3] – this includes assessing risks of components no longer being available and systematic repeatable vulnerability response processes.

8.1.2 Data asset security

8.1.2.1 General requirements

BDSPs shall:

– establish data asset security management strategies, clarify targets and principles of data asset security management;
– establish security management mechanisms and procedures covering the data asset lifecycle;
– establish data asset classification and gradation methods, and operation guidance according to the value and significance of data assets;
– establish change approval mechanisms for data classification and gradation strategies, procedures, methods, and operation guidance;
– establish security specifications, management mechanisms and procedures for data asset confidentiality, integrity and availability, (e.g., password strategy, key management);
– establish a data asset list, identify the data security responsibility issue and relevant parties;
– perform regular audits and updates on data asset security management strategies and relevant procedures.

8.1.2.2 Enhancement requirements

BDSPs should:

– establish security governance principles and data integration policies for all kinds of internal and external data resources;
– establish corresponding label, multi-level access control, data encryption and decryption, data desensitization, and other security strategies in accordance with data asset sensitivity.

8.1.3 Data supply chain process security

8.1.3.1 General requirements

BDSPs shall:

– clarify objectives, principles and scope of data supply chain security management;
– develop data supply chain security management policies and procedures, including security management criteria of data supply chain participants;
– specify purposes, supply patterns and participants' security responsibilities for data in the data supply chain by cooperation agreements;

– register equipment and applications of data acquisition and dissemination, record and audit data acquisition and dissemination behaviours;
– audit data consumption behaviours of data supply chain participants;
– establish a data source normalization mechanism and interface specification in the data supply chain, log and audit important operations;
– establish the organizational structure of supply chain operation and management, supply chain main data model, data quality processing mechanism and data traceability mechanism;
– clarify data supply chain security responsibilities, ensure authenticity and availability of related data services;
– ensure that security measures are deployed in data supply processes, e.g., data exchange and data use;
– establish data supply chain catalogues and data source dictionaries, identify the party responsible for data supply process security.
– ensure trustworthiness of records throughout the chain of provenance processing;
– clarify responsible entities for data provenance processing;
– implement authentication mechanisms to ensure authenticity of entities in the chain of processing and exchange of the provenance data;
– ensure authenticity of codes for data provenance and maintain authenticity through code updates;
– ensure the confidentiality, integrity and availability of provenance data – such security requirements are described in [ITU-T X.1601].

8.1.3.2 Enhancement requirements

BDSPs should:

– specify data service capability requirements for different data supply chain participants according to their respective roles in the ecosystem of the data business chain;
– regularly examine data security management capability of data supply chain participants, and evaluate their security risk;
– regularly evaluate security risk of the whole lifecycle of the data supply chain.

8.1.4 Metadata security

Relevant cloud service customer (CSC) data security requirements, as specified in [ITU-T X.1641], should be taken into consideration.

8.1.4.1 General requirements

BDSPs shall:

– establish data dictionaries and relevant management practices according to enterprise architecture and data services, including data domain, field type, table structure, as well as the logical and physical storage mode;
– establish security metadata and relevant management practices according to big data security architecture, including password policy, an authority list and authorization specifications;
– establish a metadata access control strategy, specify metadata roles and authorization control mechanisms;
– establish metadata operation audit procedures.

8.1.4.2 Enhancement requirements

BDSPs should:

– build metadata management systems to perform unification management of big data service metadata;
– establish an automatic grading mechanism for metadata security attributes according to the classification and grading strategy of assets;
– establish a label strategy, including the binding of data and data owner, according to metadata security requirements.

8.2 Security measures for big data applications

8.2.1 Platform resource acquisition

8.2.1.1 General requirements

BDSPs shall:

– ensure that big data service users (BDSUs) are aware and notified of system assets to be accessed by an application, such as a network connection, location service and hardware resource list like a universal serial bus (USB) and Bluetooth;
– ensure that BDSUs are aware and notified of system sensitive data assets to be accessed by an application, such as address books, system logs and other sensitive information sources;
– ensure that an application requesting access to resources has sufficient reason to visit as specified in documents provided by the application developer.

8.2.1.2 Enhanced requirements

BDSPs should:

– ensure that an application limits unnecessary internal and external network communications or user-initiated network communications based on business requirements.

8.2.2 Authorization and access control

8.2.2.1 General requirements

BDSPs shall:

– establish physical and logical access authorization granularity, specification and control mechanism of big data applications, to ensure that accesses to big data service-related data and system assets are properly authorized;
– set up authorization and access control measures based on asset management strategies and asset labels, security attributes, to ensure that a big data application has the abilities of fine-grained access control management;
– develop an information flow control strategy to control data import, export and sharing operations of the big data infrastructure between different big data applications or the big data application and external IT system;
– implement properly approved authorization of data and system asset access of individuals, groups, roles, devices and applications related to big data services;
– provide ability of an authorization access strategy self-defined by the user based on service requirements, and audit authority granted by each user based on service requirements, to ensure that its access is limited to the minimum range that meets the service scenario requirements.

8.2.2.2 Enhanced requirements

BDSPs should:

– monitor and control remote access sessions automatically to detect network attacks and ensure realization of remote access policy;

– provide an attribute-based access control (ABAC) engine and functions of authorization management and access control oriented to data objects, as well as functions like a policy administration point, policy decision point, policy enforcement point and policy access point.

8.2.3 Application behaviour monitoring

8.2.3.1 General requirements

BDSPs shall:

– establish strategies and procedures of big data application behaviour monitoring covering the whole data lifecycle;

– support users to customize monitoring rules that can support monitoring and reporting of anomalous operations on critical data;

– have ability to record, tally and analyse abnormal behaviour information about the application.

8.2.3.2 Enhanced requirements

BDSPs should:

– establish application behaviour monitoring management mechanisms oriented to regulators and users with specific requirements, and provide an online monitoring interface after authorization;

– establish a platform to record and analyse big data application behaviour, and provide security analysis capabilities providing user behaviour identification and extraction components or interfaces for big data service communication protocols;

– provide behaviour monitoring specification systems and operation guidelines.

8.2.4 Application security strategies and procedures

BDSPs shall:

– establish a release management policy for big data service applications in a written authorization procedure and responsibilities of relevant roles – the authorization document should state the name, version, source, developer, function, deployment location, security evaluation result and specific security requirements for applications;

– specify protection of data transmission between applications and big data infrastructure, as well as other authentic IT products, e.g., apply security schemes like secure socket layer (SSL), transport layer security (TLS) to encrypt sensitive data in transmission;

– check electronic signatures of application installation packages and update packages;

– ensure that an application can query the current version of running software either autonomously or by utilizing relevant big data infrastructure functions;

– ensure that an application can handle predictable error operations without affecting the normal work of big data ecosystems;

– establish a big data application update and patch management policy, ensure that applications will check for updates and install component patches;

– follow security design specifications of big data applications, avoiding entries that violate or bypass security rules and unspecified entries;

– design mechanisms to prevent vulnerability exploitation of big data applications, e.g., avoid allocating memory space that has both write and execute permissions, allocate memory space with write and execute permissions only for just-in-time compilation functions.

8.2.5 Credential storage

8.2.5.1 General requirements

BDSPs shall:

– specify an application identity credential persistent storage method, including using a platform function instead of storage to store all identity credentials securely or the application itself realizes the function of identity credential secure storage;

– clarify credential information of an application, e.g., key, public key infrastructure (PKI), private key or password;

– clarify security protection methods and control measures to collect, store, and use personally identifiable information (PII);

– establish an evaluation process for credential storage method of an application to ensure that it meets security strategies and procedure requirements for big data service systems.

8.2.5.2 Enhanced requirements

BDSPs should:

– ensure the purpose and methods of identity credential persistent storage are listed in security specification documents.

8.2.6 Identity and authentication

8.2.6.1 General requirements

BDSPs shall:

– offer capability to manage user identity, automatically to determine user identity information in big data applications to ensure mapping relations between user identification and application layer authorization information;

– authenticate user identity using more than one authentication technique for operation of important data or important modules;

– display potentially useful usage information of big data system services available to the public, e.g., display of the last login date and time or the most recent login location.

8.2.6.2 Enhanced requirements

BDSPs should:

– authenticate user identity using more than one authentication technique in all applications for a user in a key position with at least one technique based on a biometric or digital certificate method;

– use federation-like security assertion markup language (SAML) to specify identity and role, add security and privacy requirements, thus supporting multiple identities to access big data services.

8.2.7 Default configuration security

BDSPs shall:

– ensure, when using default identity credentials or when no identity credential is configured, that an application can only provide essential functions for configuring a new identity, e.g., if using a default password to log in, a user is only permitted to enter the password modification interface and the application should not provide any other function until the default password is changed;

– for applications, provide a more secure functional module and enable security configurations of a higher security level in default installation mode, e.g., if an application can provide a

password login module and digital certificate module at the same time, in the case of a default installation mode, the application chooses to install the digital certificate module;

– limit default access permissions for a default user of the application, e.g., prevent a user with non-root minimum permission from starting a program by default;

– ensure that an application starts the user account security configuration function by default, including password length, password complexity, service life limit and account lock strategy;

– ensure initiation of necessary log audit functions, e.g., component installation update or parameter modification, when an application is installed in the default configuration.

8.2.8 Data import and export

8.2.8.1 General requirements

BDSPs shall:

– formulate data import and export strategies and procedures by taking into account factors such as storage capacity, data volume growth speed, business requirement, storage medium and performance, to prevent important data loss and reduce data loss damage;

– establish data export management strategies and mechanisms, data import and export security evaluation mechanisms and an authorization approval process;

– establish identification specifications for an exported data storage medium – the identification shall conform to unified naming rules, indicate medium numbers, export time, valid term and other important information;

– provide various data import and export methods of multi-granularity, e.g., granularity of database, model and user-specified object;

– perform imported and exported data result inspection, ensure data integrity and validity;

– record data import and export operating information, e.g., operation information, operation cycle, medium number, medium volume, transfer and storage situation, and relevant change record maintenance;

– adopt encryption mechanisms, access control and other technical measures to ensure confidentiality, integrity and availability of exported data;

– regularly verify integrity and availability of exported data.

8.2.8.2 Enhancement requirements

BDSPs should:

– capture the index parameter calculation basis of automatic data backup management, including mean time to failure, mean time to restore and mean time between failures, configure corresponding automatic data import and export software;

– possess remote data online import and export ability, regularly and semi-automatically perform user data remote storage;

– automatically back up data recombination and compression in accordance with data popularity, etc., ensure availability of massive data;

– possess an automatic compression storage function for user backup data according to data backup and restore frequency.

8.3 Security measures for interface

8.3.1 General requirements

BDSPs shall:

– provide system administrator, security administrator, security auditor and other user role interfaces and regulatory role interfaces;
– specify security requirements and security control measures for each role interface, e.g., identity authentication, authorization access, signature, time stamp and security protocol;
– specify security restrictions for using each class of interface, such as remote connections whose functions and permissions are limited;
– clarify service interface security specifications, including interface name, interface parameters and interface security requirements – the specifications provide restrictions on insecure input parameters and have ability to handle exceptions;
– provide capability to audit interface access behaviours and configurable data service interfaces;
– adopt security mechanisms, such as secure channel or encrypted transfer, to secure cross-domain security interfaces.

8.3.2 Enhanced requirements

BDSPs should:

– support audit requirements in the process of interface access, and provide necessary audit and regulatory functions for interface access;
– adopt encryption transmission method for interface transmission across security domains in the system;
– perform essential automatic monitoring and processing on interface access.

8.4 Security measures for big data as a service ecosystem

8.4.1 Security planning

The security planning stage is further divided into three sub-stages:

– requirement analysis – at which business and security requirements are identified, clarified and defined;
– solution design – at which security solution(s) are designed;
– solution evaluation – at which security solution(s) are evaluated.

After the last sub-stage, the BDSP can either go to the security construction stage for implementation or back to the solution design sub-stage for adjustment or improvement.

8.4.1.1 Requirement analysis

8.4.1.1.1 General requirements

BDSPs shall:

– determine the scope of big data service business activities and corresponding security baseline requirements for big data infrastructure;
– identify specific security threats, vulnerabilities and security risks confronted by big data infrastructure, then clarify technical and management measures for big data services;
– identify security requirement implementation priorities for the big data infrastructure.

8.4.1.1.2 Enhanced requirements

BDSPs should:

– establish security requirement analysis and review management procedure and ensure that security requirements for a big data infrastructure have integrity and are reasonable.

8.4.1.2 Solution design

8.4.1.2.1 General requirements

BDSPs shall:

– create security technical specifications of big data infrastructure and describe the security function, interface and parameters clearly.

8.4.1.2.2 Enhanced requirements

BDSPs should:

– demonstrate effectiveness of security technical specifications and ensure that the security mechanism cannot be bypassed in the implementation mechanism;

– update a security solution in a timely fashion if requirements change or technology improves until solution evaluation is completed.

8.4.1.3 Solution evaluation

8.4.1.3.1 General requirements

BDSPs shall:

– review security proposal for a big data infrastructure regularly, including security architecture and security baselines, while ensuring security requirements are fulfilled.

8.4.1.3.2 Enhanced requirements

BDSPs should:

– establish a security evaluation system and determine a set of key evaluation factors.

8.4.2 Security construction

8.4.2.1 Security architecture

8.4.2.1.1 General requirements

BDSPs shall:

– establish big data service security architecture and ensure validity of design process and realization of big data security services as described in the security architecture;

– ensure that the security domain described in security architecture documents is consistent with big data application and security functional architecture requirements;

– ensure that security architecture documents describe a security function initialization process in big data applications and on big data infrastructure, thus providing security of initialization of the platform and applications.

8.4.2.1.2 Enhancement requirements

BDSPs should:

– ensure that information in security architecture description documents is sufficient to certify that a big data service security function is able to protect itself from tampering by untrusted subjects;

– ensure that security architecture description documents provide sufficient analysis to prove that the designed mechanism of a big data service security function cannot be bypassed, and the security functions provided for a big data system have been correctly realized.

8.4.2.2 Functional specification

8.4.2.2.1 General requirements

BDSPs shall:

– provide functional specifications that are accurate and complete, and clarify mapping between functional specifications and big data service security function requirements;

– ensure that the functional specification provided integrally describes big data service security functions, and clarifies involved data supply chain relationship and service components;

– ensure that the functional specification provided describes the design objective and employment method of all big data service security function application interfaces and provides all related parameters of the security function interfaces.

8.4.2.3 Security deployment

8.4.2.3.1 General requirements

BDSPs shall:

– establish a security delivery process for application delivery from developers to a big data service system;

– describe the controlled function and authority of each role of big data service in a security deployment process;

– describe available functions and interfaces for each role of big data service, indicate a security value appropriately, especially for all security parameters controlled by users;

– describe every user role of big data service and ensure that security policies described in security policies and specifications that are necessary for operating environment security are sufficiently realized.

8.4.2.4 Boundary protection

8.4.2.4.1 General requirements

BDSPs shall:

– plan a security domain and security defence boundary consistent with the security level, including security control policies and management policies;

– plan a security domain and security defence boundary related to business control and application isolation, including security control policies and management policies;

– deploy security protection facilities at a security domain boundary, to detect and protect against abnormal incidents, potential violation, etc.;

– adopt comparative strict security defence mechanisms between security domains, e.g., identity authentication, connection management, network access control security policy, intrusion prevention, information filtering and boundary integrity check;

– develop a management policy for security defence facility updates and adopt necessary methods to ensure implementation of the policy.

8.4.2.4.2 Enhancement requirements

BDSPs should:

– provide personalized multi-tenant boundary protection measures and mechanisms;

– specify a security domain or subdomain, a data isolation mechanism between security domains and an access control mechanism for authorized users or roles.

8.4.2.5 Document management

8.4.2.5.1 General requirements

BDSPs shall:

– in a big data service system, implement document management, whose scope includes organizational strategies, rules and policies, system schemes and implementation manuals;

– determine creation, review, approval, release and archival processes for documents, clarifying corresponding security responsibilities in each document management process;

– determine storage medium and time requirements for documents, ensuring their availability and completeness;

– regularly review, update, approve and release documents, ensuring that users are updated about their latest versions;

– assign responsible agencies to establish and maintain a document management system, and put them in charge of document version change maintenance;

– manage classification of system documents.

8.4.2.5.2 Enhancement requirements

BDSPs should:

– provide a platform to manage documents within a service provider, assigning different viewing permissions according to different roles;

– ensure necessary update and version identification of corresponding documents when updating products or services.

8.4.3 Security operation

8.4.3.1 System configuration management

8.4.3.1.1 General requirements

BDSPs shall:

– formulate and perform system configuration management procedures, establish system configuration management organization structure, clarify roles and responsibilities of configuration managers, e.g., system administrators, system operators, system security officers, system auditors, database administrators and other roles;

– in accordance with business requirements and management objects, stipulate approval, operation and audit processes for configuration management, e.g., host configuration items, network configuration items, application service modules and other system configuration identifications, content configurations and relevant change activities;

– in accordance with evaluation results, formulate a big data system security function baseline configuration list and daily configuration check content list, performing necessary configuration for big data system security functions according to the principle of least privilege;

– in accordance with a big data service level agreement, configure IT product parameters in a big data system, record and maintain current security configuration information about the big data system;

– in accordance with use strategies, restrict strategies and authorization policies of purchased software, forbid or restrict software from using particular functions, ports, protocols or services of a big data system;

– clarify a controlled configuration list that requires regular change, and regularly update important configuration items of a big data system related to information security, e.g., virus database, intrusion-detection rule database, firewall rule database and vulnerability database;
– review submitted changes to big data system-controlled configurations, and approve or reject them according to security impact analysis results, record change decisions;
– restrict system developers and integrators from directly changing a big data system, relevant hardware, software and firmware in production environment, audit configuration and change events;
– before configuring or changing, test, validate and record controlled configuration and change items, and analyse system change items to estimate their potential impact on big data service security;
– monitor configuration setting parameter changes, and reasonably enable monitor, warn, defence and other functions of security equipment;
– provide relevant response measures to deal with unauthorized changes, including change-related personnel, recovery of an established configuration or interruption of affected information system operation in extreme situations.

8.4.3.1.2 Enhancement requirements

BDSPs should:

– perform configuration management effect risk evaluation regularly or at the time when significant change occurs to business or system architecture, revise baseline configuration requirements and configuration contents in accordance with evaluation results, e.g., evaluate risks and revise configuration requirements at least once a year;
– evaluate risk evaluation strategy and its effects regularly or at the time when significant change occurs to business or system architecture – according to evaluation results, revise system configuration management procedures, adjust organization management structure, configure management process, etc.;
– regularly review big data system configurations to identify unnecessary or insecure functions, ports, protocols or service configuration items;
– employ system configuration tools or automatic mechanisms to centralized management, application and verification of parameters of configuration items;
– be able to note in real time changes to big data infrastructure and virtual resource status, possess automatic adjustment ability for system service security strategy configuration.

8.4.3.2 Employment of third party services

8.4.3.2.1 General requirements

BDSPs shall:

– establish a security management policy for third party service partners;
– establish an admittance, assessment and scoring mechanism for third party service providers;
– sign service component cooperation agreements with third party service providers, clarify their obligations and responsibilities, e.g., avoid too much involvement of third party service providers in security operation of a big data system;
– ensure third party service components understand information security measures of the big data system, correctly implement required security measures and pass tests of third party evaluation agencies;
– establish component employment security policies with third party service providers, clarify employment conditions and the scope of access by external components;

– adopt necessary technical or security management measures to ensure that big data users are authorized and enabled to access system and data resources via external service components;
– audit information, such as users, intended and actual operations of external service components, and ensure traceability of big data services.

8.4.3.2.2 Enhancement requirements

BDSPs should:

– evaluate qualifications and security capabilities of third party service providers, and establish a cooperative emergency response mechanism with external service component providers;
– ensure that external service components realize security measures required by information security strategy and security plan of a big data system correctly, and pass tests of third party evaluation agencies;
– restrict use of sensitive data resources in external service components by authorized personnel, including storage medium, data files and other data resources controlled by BDSPs.

8.4.3.3 Information technology supply chain security

8.4.3.3.1 General requirements

BDSPs shall:

– establish IT supply chain security policies and procedures, clarify the filtering mechanism, filtering index and evaluation method;
– clarify roles and operations of IT supply chain participants related to data acquisition and system services;
– adopt necessary technical and management measures for substitution of the supply chain, ensure an effective response if supply chain incidents occur.

8.4.3.3.2 Enhancement requirements

BDSPs should:

– establish a data aggregation information chain model, including data extraction, integration and optimization of supply chain data source;
– establish an examination and evaluation mechanism for the supply chain, perform regular risk evaluation and security assessment, e.g., at least once a year;
– establish a data supply chain quality management and evaluation feedback mechanism.

8.4.3.4 System patch management

8.4.3.4.1 General requirements

BDSPs shall:

– establish patch management procedures, including downloading, testing, analysis, distribution, installation, archiving and other processes and content, and ensure normalized system patch management;
– set up a patch management team, keep up with vulnerability disclosure information and responses to security events, perform patch downloading, testing, installation and other tasks according to an appropriate schedule;
– establish a system patch distribution and management framework, clarify patch downloading and update mechanisms, e.g., patch management triggered by system security events, or periodically by set interval;

– possess patch compatibility testing ability before patch deployment and installation, record issues during patch update processes;
– possess a patch check function, verify that a patch is installed successfully.

8.4.3.4.2 Enhancement requirements

BDSPs should:

– establish a patch management system, update the system and install patches via software.

8.4.3.5 Business continuity plan

8.4.3.5.1 General requirements

BDSPs shall:

– regularly evaluate risks due to ongoing business, and inform users about relevant risks;
– formulate and implement an appropriate disaster backup plan in accordance with business strategic goals, clarifying level, disaster recovery requirement and recovery strategy of system disaster recovery abilities;
– regularly perform business impact analysis and risk evaluation, implement relevant business continuity training.

8.4.3.5.2 Enhancement requirements

BDSPs should:

– regularly perform a system switching experiment for relevant infrastructure of involved big data service, optimize data and system resource backup schemes according to actual requirements;
– perform a business continuity plan drill to examine integrity, operability and effectiveness of the business continuity plan, verify business continuity and system asset availability.

8.4.4 Security audit

BDSPs should carry out regular security audits over the whole BDaaS ecosystem. Audits can be executed by an internal independent audit team or third party auditors (acting as big data service partners (BDSNs)). Audit results should be appropriately visible to BDSUs.

8.4.4.1 Audit strategy management

8.4.4.1.1 General requirements

BDSPs shall:

– formulate audit strategies and procedures covering big data system behaviour and big data service data activities, including audit target, audit object, audit operation, audit method, audit frequency, relevant roles and responsibilities, management commitment, the participant coordination of supply chain and compliance analysis;
– formulate a change management process for audit strategies and procedures, record in detail the start-stop status of audit strategies and procedures, change performance policy, change description, etc., regularly review and update audit strategies and procedures;
– clarify privileges and responsibilities of users in audit strategies and procedures, establish relevant privilege grant procedure of audit strategies and procedures, audit strategy performance and audit data management roles.

8.4.4.1.2 Enhancement requirements

BDSPs should:

– establish data supply chain security audit procedures and coordination mechanisms, ensure traceability of audit events;

– regularly check and evaluate implementation of audit strategies and procedures;

– set up independent system security auditors, who should conduct regular security audits on big data service;

– possess compliance analysis technologies and tools for audit strategies and procedures based on audit data.

8.4.4.2 Audit data generation

8.4.4.2.1 General requirements

BDSPs shall:

– formulate audit data record regulation, clarify audit data organizational structure and format;

– clarify auditable events related to big data system actions, e.g., user login, account management, guest access, strategy change, privileged function authorization, service module update;

– clarify auditable events related to big data service data activities, e.g., data collection, data access, data storage, data transfer, data processing, data maintenance and data destruction;

– ensure the audit data record at least includes operation time, operation subject, operation type, operation object and operation results;

– possess fine-grained audit abilities for data operations and system service actions.

– maintain dependable time mark for audit record. Time granularity should satisfy audit requirements;

– possess abilities of auditable event selection and examination;

– regularly maintain data record policies, auditable events and audit record.

8.4.4.2.2 Enhancement requirements

BDSPs should:

– provide system interfaces for third party audit data access;

– adopt cryptography technologies to ensure non-repudiation of audit data.

8.4.4.3 Audit data protection

8.4.4.3.1 General requirements

BDSPs shall:

– provide persistent massive audit data security storage management methods and mechanisms;

– possess access authorization abilities for audit data, authorize audit data access authorities to specified audit administrators;

– adopt security technologies or control measures to ensure authenticity of audit data;

– provide an audit data archiving function, support audit data offline encryption storage methods and mechanisms;

– provide management strategies and methods for audit data storage effectiveness, data compression, etc;

– enhance audit data access management, record all operations for audit data;

– possess desensitization ability for exported audit data;
– ensure the effectiveness of a stored audit record if audit storage is exhausted, invalidated or under attack.

8.4.4.3.2 Enhancement requirements

BDSPs should:

– possess remote disaster recovery and backup ability;
– be able to provide evidence to prove authenticity and completeness of audit data provided.

8.4.4.4 Audit analysis report

8.4.4.4.1 General requirements

BDSPs shall:

– formulate audit, analysis and report strategies and procedures for audit records;
– examine and analyse audit records regularly, generate an audit analysis report;
– distribute an analysis report to specified responsible staff in an organization, if any major security hazard or illegal behaviour is discovered during audit, report to organization managers as soon as possible.

8.4.4.4.2 Enhancement requirements

BDSPs should:

– monitor and analyse auditable events in real time, to support monitoring of and response to suspicious actions;
– possess correlation analysis abilities of audit records from different sources.

Bibliography

[b-ITU-T M.3030] Recommendation ITU-T M.3030 (2002), *Telecommunications markup language (tML) framework*.

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

[b-ITU-T Y.3602] Recommendation ITU-T Y.3602 (2018), *Big data – Functional requirements for data provenance*.

[b-NIST SP 800-30] Special Publication NIST SP 800-30 (2012), *Guide for conducting risk assessments*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2021