国　际　电　信　联　盟

ITU-T X.1750

(09/2020)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

数据安全 – 大数据安全

面向大数据服务提供商的大数据即服务安全导则

ITU-T X.1750 建议书

ITU-T X 系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
消息处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务（1）	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议（1）	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1360–X.1369
智能交通系统（ITS）安全	X.1370–X.1389
分布式账簿技术安全	X.1400–X.1429
分布式账簿技术安全	X.1430–X.1449
安全协议（2）	X.1450–X.1459
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	X.1640–X.1659
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	
术语	X.1700–X.1701
量子随机数发生器	X.1702–X.1709
QKDN安全框架	X.1710–X.1711
QKDN安全设计	X.1712–X.1719
QKDN安全技术	X.1720–X.1729
数据安全	
大数据安全	**X.1750–X.1759**
5G 安全	X.1800–X.1819

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1750 建议书

面向大数据服务提供商的大数据即服务安全导则

摘要

如ITU-T Y.3600建议书所述，大数据即服务（BDaaS）是一种类别的云服务，为云服务客户提供收集、存储、分析、可视化和管理大数据的能力。随着数据量的显著增长和大数据业务的快速发展，大数据基础设施已成为提供BDaaS的核心设施。因此，BDaaS面临重大安全问题。例如，开源大数据软件设计有时无法从一开始就考虑到了安全性。大数据分析引入的新技术也可能导致传统安全保护措施的失败。ITU-T X.1750建议书分析BDaaS面临的安全挑战、确定提供BDaaS的安全方面作用和责任以及大数据基础设施的安全框架。本建议书还规定了与BDaaS相关的服务和构成成分应满足的安全保护措施。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1750	2020-09-03	17	11.1002/1000/14266

关键词

大数据即服务、安全导则、安全措施。

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一ID，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联已收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1750 建议书

面向大数据服务提供商的大数据即服务安全导则

1 范围

本建议书分析大数据即服务（BDaaS）面临的安全挑战，并为大数据服务提供商（BDSP）提供确保BDaaS安全的导则。建议书确定了提供BDaaS安全的各方的作用和责任，并为大数据基础规定了安全框架，包括平台、应用、分析、接口和BDaaS生态系统。本建议书还规定了针对与BDaaS相关的活动或成分应采取的安全保护措施。

本建议书对BDaaS实施的安全要求做出高层面描述，重点是BDaaS。BDaaS涉及大数据基础设施提供商（BDIP）和大数据应用提供商（BDAP）。因此针对BDIP和BDAP的导则和BDaaS实施详细指南不在本建议书的讨论范围之内。

2 参考文献

下列ITU-T建议书和其他参考文献的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献均会得到修订，因此本建议书的使用者应查证是否有可能使用下列建议书和其他参考文献的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用某个文件，并非意味着该文件作为单独文件出现时具备建议书的地位。

[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 定义

3.1 他处定义的术语

本建议书采用下列他处定义的术语：

3.1.1 大数据（big data）[ITU-T Y.3600]：一种范式，用于实现具有异构特性的大量数据集的收集、存储、管理、分析和视像化（可能在实时约束下）。

注 – 数据集特性示例包括大数量、高速度、高多样性等。

3.1.2 大数据即服务（big data as a service (BDaaS)）[ITU-T Y.3600]： BDaaS是一种云服务类别，其中向云服务客户提供的能力为采用大数据技术收集、存储、分析、视像化并管理数据的能力。

3.1.3 大数据来源（big data provenance）[b-ITU-T Y.3602]：根据大数据生态系统中的数据寿命周期操作，记录数据历史路径的信息。

3.1.4 云计算（cloud computing）[b-ITU-T Y.3500]：有助于网络以按需自助方式调配和管理获取一系列可伸缩和富有弹性的、可共享的物理或虚拟资源的范式。

3.1.5 云服务（cloud service）[b-ITU-T Y.3500]：通过使用定义的接口启动的、由云计算实现的一种或多种功能。

3.1.6 元数据（**metadata**）[b-ITU-T M.3030]：描述其他数据的数据。

3.1.7 安全挑战（security challenge）[ITU-T X.1601]：云服务的本质和运行环境产生的直接安全威胁以外的安全“困难”，包括“间接”威胁。

3.1.8 威胁（threat）[ISO/IEC 27000]：可能对系统或组织造成伤害的有害事件的潜在起因。

3.1.9 漏洞（vulnerability） [b-NIST-SP-800-30]：可由威胁来源加以利用的信息系统、系统安全程序、内部控制或实施中存在的弱点。

3.2 本建议书定义的术语

本建议书定义了下列术语：

3.2.1 数据资产（data asset）：由组织拥有或控制的、用电子手段记录的数据资源。

4 缩写词和首字母缩略语

本建议书使用下列缩写词和首字母缩略语：

API 应用编程接口

ABAC 基于属性的访问控制

BDaaS 大数据即服务

BDAP 大数据应用提供商

BDIP 大数据基础设施提供商

BDSN 大数据服务伙伴

BDSP 大数据服务提供商

BDSU 大数据服务用户
CSC 云服务客户
DP 数据提供商
IT 信息技术
PII 个人可识别信息
PKI 公共密钥技术设施
SAML 安全断言标记语言
SDK 软件开发工具包
SSL 安全套接层
TLS 传输层安全
USB 通用串行总线

5 惯例

本建议书中：

关键短语“**要求**”表示必须得到严格遵守的要求，且如果声称遵守本建议书，则不得与该要求有任何偏差。

关键短语“**建议**”表示是一项建议的并非需绝对遵守的要求，因此声称遵守本文件时不一定按照该要求行事。

关键短语“**禁止**”表示必须得到严格遵守的要求，且如果声称遵守本建议书，则不得与之有任何偏差。

关键短语“**作为选择可以**”表示允许的一项可选择的要求，不含有任何被建议的意思。该术语并非意味着厂商在实施中一定提供这一可选功能，网络运营商/服务提供商可作为选择提供这一功能。相反，其含义是厂商可以作为选择提供这一功能，同时仍然声称遵守本建议书提出的规范。

6 大数据即服务面临的安全威胁和挑战

本节阐述BDaaS面临的安全威胁和挑战。基于云计算的BDaaS在[ITU-T Y.3600]中阐述。应针对BDaaS考虑[ITU-T X.1601]第8节所述的与云计算环境相关的安全挑战。本建议书还描述BDaaS特定能力和服务的安全威胁和挑战，即大数据平台即服务和大数据相关软件即服务（认识到BDaaS生态系统包括数据提供商（DP）、BDAP和BDIP），包括：

– 大数据基础设施的脆弱性和安全措施的失败；
– 非结构化数据带来的存储和审计问题；
– 应用程序、平台和服务流之间接口的安全性和监管；
– 其他安全问题，例如信任、认证和视像化。

图6-1显示BDaaS安全挑战的体系结构。

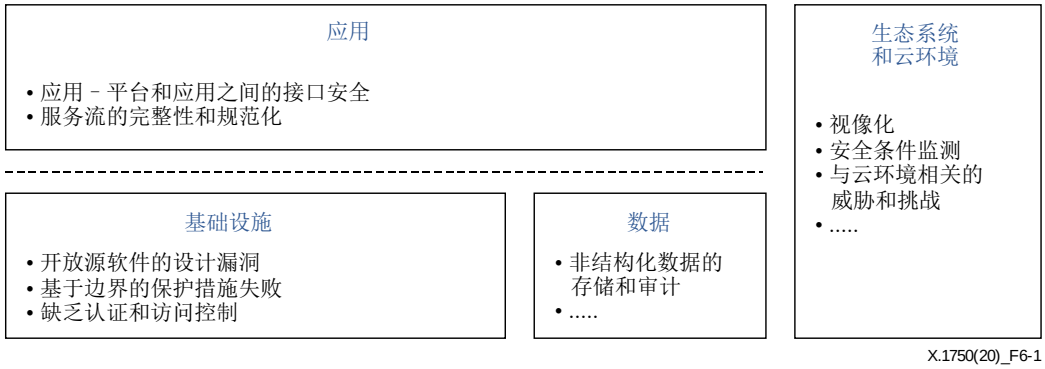

图6-1 – 大数据即服务的安全挑战

6.1 大数据基础设施的安全挑战

大数据基础设施可包含各种商业或开源组成成分。其中一些成分的设计可能从一开始就没有考虑到安全性，从而导致潜在的安全风险，包括：

– 不安全的源代码和开放源代码成分中缺乏安全机制；

– 开放和域间平台的特点模糊了传统的安全边界，导致基于边界的保护措施失败；和

– 缺乏不同角色的适当认证和访问控制机制可能会导致滥用。

6.2 大数据应用的安全挑战

大数据基础设施集成各种高度集中的应用和复杂的服务模式。大数据应用面临的安全挑战包括：

– 应用编程接口（API）、软件开发工具包（SDK）和应用之间的接口可能缺乏安全验证和传输控制；和

– 跟踪、审计和定位用户应用的执行情况，以保证服务逻辑安全的必要性。

6.3 数据的安全挑战

大数据基础设施和应用处理大量数据。在大数据生态系统中，数据类型包括结构化、半结构化和非结构化数据。结构化数据通常存储在可组织成不同模式的数据库中，如关系、文档、键值（key-value）、图形等模式。半结构化数据不符合数据模式的形式结构，但包含标识数据的标签或标记。非结构化数据没有预定义的数据模式，也没有以任何既定的方式组织。在所有数据类型中，数据可以以不同的格式存在，如文本、电子表格、视频、音频、图像、地图等（见[ITU-T Y.3600]）。这些数据用于存储、分析、计算和其他数据服务阶段。数据的安全挑战包括：

– 要求采取安全措施（包括访问控制），以确保数据保密性，同时仍然支持有效的数据操作；

– 非结构化数据的审计；

– 如果数据是公开的或共享的，个人隐私信息存在泄露风险；

– 在元数据具有与网上发布的数据相同的特性时，应用 [ITU-T X.1601]描述的传统安全措施的必要性；

大数据来源处理面临的安全挑战包括：整个来源处理链中被污染或被恶意篡改的记录、来源数据处理或交换中未经授权的实体、数据来源处理的不真实代码，以及来源数据面临的安全挑战。

6.4 大数据即服务生态系统的安全挑战

根据[ITU-T Y.3600]，BDaaS生态系统由提供和消费大数据服务的不同方或组成成分所扮演的角色和子角色组成。BDaaS生态系统需要在服务来源的建设、操作、审计和其他阶段规划、设计和实施安全措施。大数据服务面临的安全挑战包括：

– 持续监控用户行为、网络状况、资源状态等，以应对不断变化的威胁的必要性
– 新出现的威胁媒介和缺乏潜在的保护机制；
– 无法在各种行为者之间建立信任，包括数据和设备所有（收集数据）；
– 虚拟化实例化的安全性，例如安全性配置和虚拟图像完整性；
– 大数据生态系统可能由复杂的供应链组成的可能性。即使不是直接与组织签约的承包商也可能影响组织的业务连续性；
– 应分析与供应链相关的风险，并采取必要的措施，包括[ISO/IEC 27000] [ISO 28000]中描述的安全措施。

7 大数据即服务的高层面概念安全考虑和BDSP的角色

[ITU-T Y.3600]规定了大数据技术的体系结构，该体系结构是通用的、多级的，并且由逻辑功能成分组成。基于这种架构，大数据服务安全功能涵盖了系统安全和数据安全。

从系统安全的角度看，BDaaS安全需求涵盖 1) 大数据基础设施；2) 大数据应用管理；3) 接口安全；和4) 大数据平台安全的操作和维护（BDaaS生态系统）的每个相关功能模块的能力。

特别是，[ITU-T Y.3600]描述的BDaaS有两个关键组成部分：

– BDIP ： 可以使用云基础设施能力类型的云服务，如计算即服务、数据存储即服务、基础设施即服务和网络即服务，来执行收集、处理和管理方面的大数据服务；
– BDAP：BDAP将执行数据分析、可视化和其他大数据应用。

从数据安全角度看，安全要求涵盖了大数据服务服务开发过程中的每项活动。此外，大数据服务安全功能还包括元数据安全和数据供应链安全要求。

[ITU-T Y.3600]从BDaaS的系统角度确定了包括角色和活动以及数据和服务流在内的系统环境。

在[ITU-T Y.3600]角色方面，BDaaS服务由BDSP提供，后者负责确保BDaaS的安全性并降低风险。建议BDSP（BDIP和BDAP）在实施BDaaS活动时同时考虑系统安全性和数据安全性。

8 大数据即服务的安全措施

8.1 大数据基础实施的安全措施

8.1.1 系统资产安全性

8.1.1.1 一般要求

BDSP须：

- 制定系统资产安全管理战略，明确系统资产安全的具体目标和原则；
- 建立系统资产的建设和操作管理政策和程序，包括规划、设计、采购、开发、运行、维护和报废；
- 建立系统资产登记机制，制定系统资产清单，明确规定系统资产的安全责任问题和相关方，定期充实完善系统资产信息；
- 建立和实施系统资产分类和标签程序；
- 对信息技术（IT）资产和安全管理政策进行定期审计和更新。

8.1.1.2 增强要求

BDSP应：

- 确定可用的资产管理控制机制（如[ITU-T X.1631]中阐述的控制机制），以进行系统资产成分的清点和登记、审计和监督；
- 为大数据系统建立资产风险评估程序。例如，实施流程，确定对维护功能性至关重要的、因此需要更多的关注和审查的产品或服务成分；
- 建立供应链安全评估程序（如[ISO/IEC 27036-3]规定的程序）。该工作可包括评估不再可用成分的风险和对系统重复性漏洞的响应流程等。

8.1.2 数据资产安全性

8.1.2.1 一般要求

BDSP须：

- 制定数据资产安全管理战略，明确数据资产安全管理的具体目标和原则；
- 建立涵盖数据资产寿命周期的安全管理机制和程序；
- 根据数据资产的价值和重要性，建立数据资产分类和分级方法及操作指南；
- 建立数据分类和分级战略、程序、方法和操作指南的变更批准机制；
- 为数据资产的机密性、完整性和可用性建立安全规范、管理机制和程序（例如，密码战略、密钥管理）；
- 建立数据资产清单，确定数据安全责任问题和相关方；
- 对数据资产安全管理战略和相关程序进行定期审计和更新。

8.1.2.2 增强要求

BDSP应：

– 为各种内部和外部数据资源建立安全治理原则和数据集成政策；

– 根据数据资产敏感性，建立相应的标签、多级访问控制、数据加密和解密、数据脱敏等安全战略。

8.1.3 数据供应链流程安全性

8.1.3.1 一般要求

BDSP须：

– 明确数据供应链安全管理的目标、原则和范围；

– 制定数据供应链安全管理政策和程序，包括数据供应链参与方的安全管理标准；

– 通过合作协议规定数据供应链中数据的目的、供应模式和参与方的安全责任；

– 登记数据获取和传播的设备和应用，记录和审计数据获取和传播行为；

– 审计数据供应链参与方的数据消费行为；

– 在数据供应链中建立数据源规范化机制和接口规范，记录和审核重要操作；

– 建立供应链运营和管理的组织结构、供应链主要数据模式、数据质量处理机制和数据追溯机制；

– 明确数据供应链安全责任，确保相关数据服务的真实性和可用性；

– 确保在数据提供过程，例如数据交换和数据使用中部署安全措施；

– 建立数据供应链目录和数据源字典，确定负责数据供应过程安全的一方；

– 确保整个来源处理链中记录的可信度；

– 明确负责数据来源处理的实体；

– 实施认证机制，以确保处理和交换源数据链中实体的真实性；

– 确保数据来源代码的真实性，并通过代码更新保持真实性；

– 确保来源数据的保密性、完整性和可用性，此类安全要求在[ITU-T X.1601]中有所描述。

8.1.3.2 增强要求

BDSP应：

– 根据数据供应链不同参与方在数据业务链生态系统中各自的角色，为之明确规定数据服务能力要求；

– 定期检查数据供应链参与方的数据安全管理能力，并评估安全风险；

– 定期评估数据供应链整个寿命周期的安全风险。

8.1.4 元数据安全性

应考虑相关的云服务客户（CSC）数据安全要求，如[ITU-T X.1641]所述要求。

8.1.4.1 一般要求

BDSP须：

– 根据企业架构和数据服务建立数据字典和相关管理做法，包括数据域、字段类型、表结构以及逻辑和物理存储模式；

– 根据大数据安全架构建立安全元数据和相关管理做法，包括密码政策、权限列表和授权规范；

– 建立元数据访问控制战略，具体规定元数据角色和授权控制机制；

– 建立元数据操作审计程序。

8.1.4.2 增强要求

BDSP应：

– 建立元数据管理系统，对大数据服务元数据进行统一管理；

– 根据资产的分类和分级战略，建立元数据安全属性的自动分级机制；

– 根据元数据安全要求，建立标签战略，包括数据和数据所有者的绑定。

8.2 大数据应用的安全措施

8.2.1 平台资源获取

8.2.1.1 一般要求

BDSP须：

– 确保大数据服务用户（BDSU）了解并被通知将由应用访问的系统资产，例如网络连接、定位服务和硬件资源列表，如通用串行总线（USB）和蓝牙；

– 确保BDSU了解和被通知应用将要访问的系统敏感数据资产，如地址簿、系统日志和其他敏感信息源；

– 确保请求访问资源的应用有足够的理由进行访问，例如应用开发人员提供的文档中具体规定的理由。

8.2.1.2 增强要求

BDSP应：

– 确保应用根据业务要求限制不必要的内部和外部网络通信或用户发起的网络通信。

8.2.2 授权和访问控制

8.2.2.1 一般要求

BDSP须：

– 建立大数据应用的物理和逻辑访问授权粒度、规范和控制机制，确保对大数据服务相关数据和系统资产的访问得到适当授权；

– 基于资产管理战略和资产标签以及安全属性建立授权和访问控制措施，以确保大数据应用具有细粒度访问控制管理的能力；

– 制定信息流控制战略，以控制不同大数据应用或大数据应用与外部信息技术系统之间大数据基础设施的数据导入、导出和共享操作；
– 对与大数据服务相关的个人、群体、角色、设备和应用的数据和系统资产访问实施适当批准的授权；
– 提供用户基于服务要求自定义的授权访问战略能力，以及每个用户基于服务要求授予的审计权限，以确保其访问被限制在满足服务场景要求的最小范围内。

8.2.2.2 增强要求

BDSP应：

– 自动监控远程访问会话以发现网络攻击并确保远程访问政策的实现；
– 提供基于属性访问控制（ABAC）引擎和面向数据对象的授权管理和访问控制功能，以及诸如政策管理点、决策点、政策执行点和政策访问点等功能。

8.2.3 应用行为监控

8.2.3.1 一般要求

BDSP须：

– 建立涵盖整个数据寿命周期的大数据应用行为监控战略和程序；
– 支持用户定制监控规则，支持对关键数据的异常操作进行监控和报告；
– 能够记录、统计和分析应用的异常行为信息。

8.2.3.2 增强要求

BDSP应：

– 建立面向监管者和有特殊要求的用户的应用行为监控管理机制，授权后提供在线监控界面；
– 建立记录和分析大数据应用行为的平台，并提供安全分析能力，为大数据服务通信协议提供用户行为识别和提取成分或接口；
– 提供行为监控规范系统和操作指南。

8.2.4 应用安全战略和程序

BDSP须：

– 制定大数据服务应用的发布管理政策，以书面形式规定授权程序和相关角色的职责 – 授权文件应详细声明应用的名称、版本、来源、开发者、功能、部署地点、安全评估结果和具体的安全要求；
– 明确对应用和大数据基础设施以及其他真是信息技术产品之间的数据传输保，，例如，采用安全套接层（SSL）、传输层安全性（TLS）等安全方案来加密传输中的敏感数据；
– 检查应用安装包和更新包的电子签名；
– 确保应用可自主地或通过利用相关的大数据基础设施功能来查询运行软件的当前版本；

– 确保应用能够处理可预测的错误操作，而不影响大数据生态系统的正常工作；
– 建立大数据应用的更新和补丁管理政策，确保应用将检查更新并安装组件补丁；
– 遵循大数据应用的安全设计规范，避免违反或绕过安全规则的条目，以及未明确规定的条目；
– 通过设计机制防止大数据应用的漏洞被利用，例如，避免分配具有写入和执行权限的内存空间，只对即时编译功能分配具有写入和执行权限的内存空间。

8.2.5 证书凭证存储

8.2.5.1 一般要求

BDSP须：

– 明确规定应用身份证书持久存储方法，包括使用平台功能取代存储来安全地存储所有身份证书或者应用本身来实现身份证书安全存储的功能；
– 澄清应用的证书信息，例如密钥、公钥基础设施（PKI）、私人密钥或密码；
– 阐明收集、储存和使用个人可识别（PII）信息的安全保护方法和控制措施；
– 建立应用证书存储方法的评估流程，以确保其符合大数据服务系统的安全战略和流程要求。

8.2.5.2 增强要求

BDSP应：

– 确保身份证书永久存储的目的和方法在安全规范文件中列出。

8.2.6 身份和认证

8.2.6.1 一般要求

BDSP须：

– 提供管理用户身份的能力，自动确定大数据应用中的用户身份信息，以确保用户身份和应用层授权信息之间的映射关系；
– 对重要数据或重要模块的操作使用一种以上的认证技术来认证用户身份；
– 显示公众可用的大数据系统服务的潜在有用使用信息，例如，显示最近的登录日期和时间或最近的登录位置。

8.2.6.2 增强要求

BDSP应：

– 对在所有应用中处于关键位置的用户使用一种以上的身份认证技术进行身份认证，至少使用一种基于生物特征或数字证书方法的技术进行身份认证；
– 使用类似联邦的安全断言标记语言（SAML）来具体规定身份和角色、添加安全和隐私要求，从而支持多个身份获取大数据服务。

8.2.7 默认配置安全性

BDSP须：

– 当使用默认身份证书时或当没有配置身份证书时，确保应用只能提供用于配置新身份的基本功能，例如，如果使用默认密码登录，则仅允许用户进入密码修改界面，并且在更改默认密码之前，应用不应提供任何其他功能；

– 对于应用，提供更安全的功能模块，并在默认安装模式下启用更高安全级别的安全配置，例如，如果应用可以同时提供密码登录模块和数字证书模块，在默认安装模式的情况下，应用应选择安装数字证书模块；

– 限制应用默认用户的默认访问权限，例如，防止具有非根最小权限的用户默认启动程序；

– 确保应用以默认方式启动用户帐户安全配置功能，包括密码长度、密码复杂性、使用寿命限制和帐户锁定战略；

– 当应用程序以默认配置安装时，确保启动必要的日志审核功能，例如成分安装更新或参数修改。

8.2.8 数据导入和导出

8.2.8.1 一般要求

BDSP须：

– 通过考虑诸如存储容量、数据量增长速度、业务要求、存储媒介和性能等因素来制定数据导入和导出战略和程序，以防止重要数据丢失并减少数据丢失损害；

– 建立数据导出管理战略和机制、数据导入和导出安全评估机制和授权批准程序；

– 为导出的数据存储媒介建立标识规范 – 标识须符合统一的命名规则，标明媒介编号、导出时间、有效期限和其他重要信息；

– 提供多粒度的各种数据导入和导出方法，如数据库、模型和用户指定对象的粒度；

– 进行导入和导出数据结果检查，确保数据的完整性和有效性；

– 记录数据导入和导出操作信息，如操作信息、操作周期、媒介编号、媒介量、传送和存储情况，以及相关的变更记录；

– 采用加密机制、访问控制和其他技术措施，确保导出数据的保密性、完整性和可用性；

– 定期验证导出数据的完整性和可用性。

8.2.8.2 增强要求

BDSP应：

– 捕获自动数据备份管理的指标参数计算依据，包括平均故障时间、平均恢复时间和平均故障间隔时间，配置相应的自动数据导入和导出软件；

– 具备远程数据在线导入和导出能力，定期和半自动地进行用户数据远程存储；

– 根据数据流行度等因素自动备份数据重组和压缩，确保海量数据的可用性；

– 具有根据数据备份和恢复频率自动压缩存储用户备份数据的功能。

8.3 接口的安全措施

8.3.1 一般要求

BDSP须：

– 提供系统管理员、安全管理员、安全审计员和其他用户角色界面和监管角色界面；
– 为每个角色接口具体规定安全要求和安全控制措施，例如身份认证、授权访问、签名、时间戳和安全协议；
– 具体规定使用每类接口的安全限制，例如功能和权限受限的远程连接；
– 阐明服务接口安全规范，包括接口名称、接口参数和接口安全要求 – 这些规范对不安全的输入参数予以限制，并具有处理异常情况的能力；
– 提供审计接口访问行为和可配置数据服务接口的能力；
– 采用安全机制，如安全信道或加密传送，以保护跨域安全接口。

8.3.2 增强要求

BDSP应：

– 支持接口访问过程中的审计要求，并为接口访问提供必要的审计和监管功能；
– 对系统中跨安全域的接口传输采用加密传输方式；
– 对接口访问实行必要的自动监控和处理。

8.4 大数据即服务生态系统的安全措施

8.4.1 安全规划

安全规划阶段进一步分为三个分阶段：

– 要求分析 – 确定、澄清和定义业务和安全要求分阶段；
– 解决方案设计 – 设计安全解决方案分阶段；
– 解决方案评估 – 评估安全解决方案分阶段。

在此最后的分阶段之后，BDSP可进入安全构建阶段进行实施，或回到解决方案设计分阶段进行调整或改进。

8.4.1.1 要求分析

8.4.1.1.1 一般要求

BDSP须：

– 确定大数据服务业务活动的范围以及大数据基础设施的相应安全基线要求；
– 确定大数据基础设施面临的特定安全威胁、漏洞和安全风险，然后阐明大数据服务的技术和管理措施；
– 确定大数据基础设施的安全要求实施的轻重缓急。

8.4.1.1.2 增强要求

BDSP应：

– 建立安全要求分析和审查管理程序，并确保大数据基础设施的安全要求具有完整性和合理性。

8.4.1.2 解决方案的设计

8.4.1.2.1 一般要求

BDSP须：

– 创建大数据基础设施的安全技术规范，并清楚地描述安全功能、接口和参数。

8.4.1.2.2 增强要求

BDSP应：

– 表明安全技术规范的有效性，并确保在实施机制中不能绕过安全机制；
– 如果需求变化或技术改进，及时更新安全解决方案，直到解决方案评估完成。

8.4.1.3 解决方案的评估

8.4.1.3.1 一般要求

BDSP须：

– 定期审查大数据基础设施的安全建议，包括安全架构和安全基线，同时确保满足安全要求。

8.4.1.3.2 增强要求

BDSP应：

– 建立安全评估系统并确定一系列关键评估因素。

8.4.2 安全构建

8.4.2.1 安全架构

8.4.2.1.1 一般要求

BDSP须：

– 建立大数据服务安全架构，确保安全架构中描述的大数据安全服务的设计过程和实现的有效性；
– 确保安全架构文件中描述的安全域符合大数据应用和安全功能架构要求；
– 确保安全架构文件描述大数据应用和大数据基础设施的安全功能初始化过程，从而提供平台和应用初始化的安全性。

8.4.2.1.2 增强要求

BDSP应：

– 确保安全架构描述文件中的信息足以证明大数据服务安全功能能够保护自身免受不可信主体的篡改；

– 确保安全架构描述文件提供足够的分析，以证明所设计的大数据服务安全功能机制不可绕过，所提供的大数据系统安全功能已正确实现。

8.4.2.2 功能规范

8.4.2.2.1 一般要求

BDSP须：

– 提供准确完整的功能规范，明确功能规范与大数据服务安全功能要求之间的对应关系；

– 确保所提供的功能规范完整地描述大数据服务安全功能，并阐明所涉及的数据供应链关系和服务成分；

– 确保所提供的功能规范描述所有大数据服务安全功能应用接口的设计目标和使用方法，并提供安全功能接口的所有相关参数。

8.4.2.3 安全部署

8.4.2.3.1 一般要求

BDSP须：

– 为从开发人员到大数据服务系统的应用交付建立安全交付流程；

– 描述安全部署过程中大数据服务各角色的受控功能和权限；

– 描述大数据服务的每个角色的可用功能和接口，适当指明安全值，尤其是由用户控制的所有安全参数；

– 描述大数据服务的每个用户角色，并确保操作环境安全所需的安全政策和规范中描述的安全政策得到充分实现。

8.4.2.4 边界保护

8.4.2.4.1 一般要求

BDSP须：

– 根据安全级别规划安全域和安全防御边界，包括安全控制政策和管理政策；

– 规划与业务控制和应用隔离相关的安全域和安全防御边界，包括安全控制政策和管理政策；

– 在安全域边界部署安全保护设施，以发现并防止异常事件、潜在违规等；

– 在安全域之间采用相对严格的安全防御机制，例如身份认证、连接管理、网络访问控制安全政策、入侵预防、信息过滤和边界完整性检查；

– 制定安全防御设施更新的管理政策，并采取必要方法以确保政策的实施。

8.4.2.4.2 增强要求

BDSP应：

– 提供个性化的多租户边界保护措施和机制；
– 规范安全域或子域、安全域之间的数据隔离机制以及经授权用户或角色的访问控制机制。

8.4.2.5 文件管理

8.4.2.5.1 一般要求

BDSP须：

– 在大数据服务系统中实现文件管理，其范围包括组织战略、规则和政策、系统方案和实施手册；
– 确定文件的创建、审查、批准、发布和归档流程，明确每个文件管理过程中相应的安全责任；
– 确定文件的存储媒介和时间要求，确保其可用性和完整性；
– 定期审查、更新、批准和发布文件，确保用户了解最新版本；
– 指定负责机构建立和维护文件管理系统，并负责文件版本变更的充实完善；
– 管理系统文件的分类。

8.4.2.5.2 增强要求

BDSP应：

– 提供平台来管理服务提供商内的文件，根据不同的角色分配不同的查看权限；
– 在更新产品或服务时，确保相应文件的必要更新和版本标识。

8.4.3 安全操作

8.4.3.1 系统配置管理

8.4.3.1.1 一般要求

BDSP须：

– 制定和执行系统配置管理程序，建立系统配置管理组织结构，明确配置管理人员的角色和职责，例如系统管理员、系统操作员、系统安全官员、系统审计员、数据库管理员和其他角色；
– 根据业务要求和管理对象，规定配置管理的审批、运行和审核流程，如主机配置项、网络配置项、应用服务模块和其他系统配置标识、内容配置及相关变更活动；
– 根据评估结果，制定大数据系统安全功能基线配置列表和日常配置检查内容列表，按照最小特权原则对大数据系统安全功能进行必要的配置；
– 根据大数据服务水平协议，在大数据系统中配置信息技术产品参数，记录和维护大数据系统当前的安全配置信息；
– 根据使用战略、限制购买软件的战略和授权战略，禁止或限制软件使用大数据系统的特定功能、端口、协议或服务；

– 明确需要定期变更的受控配置列表，定期更新与信息安全相关的大数据系统的重要配置项目，如病毒数据库、入侵检测规则数据库、防火墙规则数据库和漏洞数据库；
– 审查提交的对大数据系统控制的配置更改，并根据安全影响分析结果予以批准或拒绝，记录更改决定；
– 限制系统开发人员和集成商在生产环境中直接更改大数据系统、相关硬件、软件和固件，审核配置和更改事件；
– 在执行配置或更改之前，测试、验证和记录受控配置和更改项目，并分析系统更改项目，以评估其对大数据服务安全性的潜在影响；
– 监控配置设置参数的变化，合理启用安全设备的监控、报警、防御等功能；
– 提供相关的响应措施，以处理未经授权的变更，包括与变更相关的人员，恢复已建立的配置或在极端情况下中断受影响的信息系统的运行 。

8.4.3.1.2 增强要求

BDSP应：

– 定期或在业务或系统架构发生重大变化时进行配置管理效果风险评估，根据评估结果修改基线配置要求和配置内容，如每年至少评估一次风险并修改配置要求；
– 定期或在业务或系统架构发生重大变化时评估风险评估战略及其效果 – 根据评估结果，修改系统配置管理程序，调整组织管理结构，配置管理流程等；
– 定期审查大数据系统配置以明确不必要或不安全的功能、端口、协议或服务配置项目；
– 使用系统配置工具或自动机制来集中管理、应用和验证配置项目的参数；
– 能够实时记录大数据基础设施和虚拟资源状态的变化，具备系统服务安全战略配置的自动调整能力。

8.4.3.2 第三方服务的采用

8.4.3.2.1 一般要求

BDSP须：

– 为第三方服务合作伙伴制定安全管理政策；
– 为第三方服务提供商建立接纳、评估和评分机制；
– 与第三方服务提供商签署服务成分合作协议，明确其义务和责任，例如，避免第三方服务提供商过多参与大数据系统的安全操作；
– 确保第三方服务成分了解大数据系统的信息安全措施，正确实施所需的安全措施，并通过第三方评估机构的测试；
– 与第三方服务提供商一起制定成分采用安全政策，明确外部成分的采用条件和访问范围；
– 采取必要的技术或安全管理措施，以确保大数据用户获得授权并能够通过外部服务成分访问系统和数据资源；
– 审核外部服务成分的用户、预期和实际操作等信息，并确保大数据服务的可追溯性。

8.4.3.2.2 增强要求

BDSP应：

– 评估第三方服务提供商的资质和安全能力，并与外部服务成分提供商一起建立合作应急机制；
– 确保外部服务成分正确实现大数据系统信息安全战略和安全计划要求的安全措施，并通过第三方评估机构的测试；
– 通过人员授权方式限制使用外部服务成分中的敏感数据资源，包括存储媒介、数据文档和由BDSP控制的其他数据资源。

8.4.3.3 信息技术供应链安全性

8.4.3.3.1 一般要求

BDSP须：

– 建立信息技术供应链安全政策和程序，明确过滤机制、过滤指标和评价方法；
– 明确与数据获取和系统服务相关的信息技术供应链参与方的角色和操作工作；
– 采取必要的技术和管理措施取代供应链，确保在供应链事件发生时做出有效响应。

8.4.3.3.2 增强要求

BDSP应：

– 建立数据汇集信息链模型，包括供应链数据源的数据提取、集成和优化；
– 建立供应链检查和评价机制，定期进行风险评估和安全评估，例如至少每年一次；
– 建立数据供应链质量管理和评价反馈机制。

8.4.3.4 系统补丁管理

8.4.3.4.1 一般要求

BDSP须：

– 建立补丁管理程序，包括下载、测试、分析、分发、安装、归档等流程和内容，确保系统补丁管理的规范化；
– 建立补丁管理团队，跟踪漏洞披露信息和对安全事件的响应，根据适当的时间表执行补丁下载、测试、安装和其他任务；
– 建立系统补丁分发和管理框架，阐明补丁下载和更新机制，例如，由系统安全事件触发的补丁管理，或以设定的时间间隔周期性地触发补丁管理；
– 在补丁部署和安装前具备补丁兼容性测试能力，记录补丁更新过程中的问题；
– 具备补丁检查功能，核验补丁安装成功。

8.4.3.4.2 增强要求

BDSP应：

– 建立补丁管理系统，更新系统并通过软件安装补丁。.

8.4.3.5 业务连续性计划

8.4.3.5.1 一般要求

BDSP须：

– 定期评估连续性业务带来的风险，并告知用户相关风险；

– 根据业务战略目标制定并实施适当的灾难备份计划，明确系统灾难恢复能力的级别、灾难恢复要求和恢复战略；

– 定期进行业务影响分析和风险评估，实施相关的业务连续性培训。

8.4.3.5.2 增强要求

BDSP应：

– 定期对涉及大数据服务的相关基础设施进行系统切换实验，根据实际要求优化数据和系统资源备份方案；

– 进行业务连续性计划演练，以检验业务连续性计划的完整性、可操作性和有效性，并核验业务连续性和系统资产可用性。

8.4.4 安全审计

BDSP应对整个BDaaS生态系统进行定期安全审计。审计可由内部独立审计团队或第三方审计员（作为大数据服务合作伙伴（BDSN））进行。审计结果应对BDSU适当可见。

8.4.4.1 审计战略管理

8.4.4.1.1 一般要求

BDSP须：

– 制定涵盖大数据系统行为和大数据服务数据活动的审计战略和程序，包括审计具体目标、审计对象、审计操作、审计方法、审计频率、相关角色和职责、管理层的承诺、供应链参与方协调和合规性分析；

– 确立关于审计战略和程序的变更管理流程，详细记录审计战略和程序的起止状态、变更执行政策、变更描述等；定期审查和更新审计战略和程序；

– 在审计战略和程序中明确用户的特权和责任，确立审计战略和程序的相关特权授予程序、审计战略执行和审计数据管理角色。

8.4.4.1.2 增强要求

BDSP应：

– 确立数据供应链安全审计程序和协调机制，确保审计事件的可追溯性；

– 定期检查和评估审计战略和程序的执行情况；

– 指定独立的系统安全审计员，负责定期对大数据服务进行安全审计；

– 拥有基于审计数据的审计战略和程序的合规性分析技术和工具。

8.4.4.2 审计数据的生成

8.4.4.2.1 一般要求

BDSP须：

- 制定审计数据记录规定，明确审计数据的组织结构和形式；
- 阐明与大数据系统操作相关的可审计事件，例如，用户登录、帐户管理、访客访问、战略更改、特权功能授权、服务模块更新；
- 澄清与大数据服务数据活动相关的可审计事件，例如数据收集、数据访问、数据存储、数据传送、数据处理、数据维护和数据销毁；
- 确保审计数据记录至少包括操作时间、操作主体、操作类型、操作对象和操作结果；
- 拥有数据操作和系统服务操作的细粒度审计能力；
- 保持审计记录的可靠时间标记。时间粒度应满足审计要求；
- 具备可审计事件的选择和审查能力；
- 定期充实完善数据记录政策、可审计事件和审计记录。

8.4.4.2.2 增强要求

BDSP应：

- 为访问第三方审计数据提供系统接口；
- 采用加密技术确保审计数据的不可否认性。

8.4.4.3 审计数据的保护

8.4.4.3.1 一般要求

BDSP须：

- 提供持久的海量审计数据安全存储管理方法和机制；
- 拥有审计数据的访问授权能力，将审计数据访问权限授予指定的审计管理人员；
- 采用安全技术或控制措施，确保审计数据的真实性；
- 提供审计数据归档功能，支持审计数据离线加密存储方法和机制；
- 为审计数据存储有效性、数据压缩等提供管理战略和方法；
- 加强审计数据访问管理，记录审计数据的所有操作；
- 对输出的审计数据具有脱敏能力；
- 如果审计存储耗尽、失效或受到攻击，确保存储的审计记录的有效性。

8.4.4.3.2 增强要求

BDSP应：

- 具备远程灾难恢复和备份能力；
- 能够提供证据证明所提供审计数据的真实性和完整性。

8.4.4.4 审计分析报告

8.4.4.4.1 一般要求

BDSP须：

– 制定审计、分析和报告审计记录的战略和程序；
– 定期检查和分析审计记录，生成审计分析报告；
– 向组织中指定的负责人员分发分析报告，如果在审计过程中发现任何重大安全隐患或违法行为，应尽快向组织管理层报告。

8.4.4.4.2 增强要求

BDSP应：

– 实时监控和分析可审计事件，以支持监控和应对可疑行动；
– 具备对不同来源审计记录予以关联性分析的能力。

参考资料

[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*.

ITU-T系列建议书

系列A	ITU-T工作的组织
系列D	资费及结算原则和国际电信/ICT的经济和政策问题
系列E	综合网络运行、电话业务、业务运行和人为因素
系列F	非话电信业务
系列G	传输系统和媒介、数字系统和网络
系列H	视听及多媒体系统
系列I	综合业务数字网
系列J	有线网络和电视、声音节目及其他多媒体信号的传输
系列K	干扰的防护
系列L	环境与ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列M	电信管理，包括TMN和网络维护
系列N	维护：国际声音节目和电视传输电路
系列O	测量设备的技术规范
系列P	电话传输质量、电话设施及本地线路网络
系列Q	交换和信令，以及相关的测量和测试
系列R	电报传输
系列S	电报业务终端设备
系列T	远程信息处理业务的终端设备
系列U	电报交换
系列V	电话网上的数据通信
系列X	**数据网、开放系统通信和安全性**
系列Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列Z	用于电信系统的语言和一般软件问题

瑞士印刷
2021年，日内瓦