



# 中华人民共和国国家标准

GB/T 37988—2019

---

## 信息安全技术 数据安全能力成熟度模型

Information security technology—Data security capability maturity model

2019-08-30 发布

2020-03-01 实施

---

国家市场监督管理总局  
中国国家标准化管理委员会 发布

## 目 次

前言 .....	III
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 缩略语 .....	3
5 DSMM 架构 .....	3
5.1 成熟度模型架构 .....	3
5.2 安全能力维度 .....	4
5.3 能力成熟度等级维度 .....	4
5.4 数据安全过程维度 .....	6
6 数据采集安全 .....	7
6.1 PA01 数据分类分级 .....	7
6.2 PA02 数据采集安全管理 .....	8
6.3 PA03 数据源鉴别及记录 .....	9
6.4 PA04 数据质量管理 .....	11
7 数据传输安全 .....	12
7.1 PA05 数据传输加密 .....	12
7.2 PA06 网络可用性管理 .....	13
8 数据存储安全 .....	14
8.1 PA07 存储媒体安全 .....	14
8.2 PA08 逻辑存储安全 .....	15
8.3 PA09 数据备份和恢复 .....	17
9 数据处理安全 .....	19
9.1 PA10 数据脱敏 .....	19
9.2 PA11 数据分析安全 .....	20
9.3 PA12 数据正当使用 .....	22
9.4 PA13 数据处理环境安全 .....	23
9.5 PA14 数据导入导出安全 .....	24
10 数据交换安全 .....	26
10.1 PA15 数据共享安全 .....	26
10.2 PA16 数据发布安全 .....	27
10.3 PA17 数据接口安全 .....	28
11 数据销毁安全 .....	29
11.1 PA18 数据销毁处置 .....	29
11.2 PA19 存储媒体销毁处置 .....	31

12 通用安全 .....	32
12.1 PA20 数据安全策略规划 .....	32
12.2 PA21 组织和人员管理 .....	34
12.3 PA22 合规管理 .....	36
12.4 PA23 数据资产管理 .....	38
12.5 PA24 数据供应链安全 .....	39
12.6 PA25 元数据管理 .....	41
12.7 PA26 终端数据安全 .....	42
12.8 PA27 监控与审计 .....	43
12.9 PA28 鉴别与访问控制 .....	44
12.10 PA29 需求分析 .....	46
12.11 PA30 安全事件应急 .....	47
附录 A (资料性附录) 能力成熟度等级描述与 GP .....	49
A.1 概述 .....	49
A.2 能力成熟度等级 1——非正式执行 .....	49
A.3 能力成熟度等级 2——计划跟踪 .....	49
A.4 能力成熟度等级 3——充分定义 .....	50
A.5 能力成熟度等级 4——量化控制 .....	51
A.6 能力成熟度等级 5——持续优化 .....	52
附录 B (资料性附录) 能力成熟度等级评估参考方法 .....	54
附录 C (资料性附录) 能力成熟度等级评估流程和模型使用方法 .....	55
C.1 能力成熟度等级评估流程 .....	55
C.2 能力成熟度模型使用方法 .....	56
参考文献 .....	57

## 前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:阿里巴巴(北京)软件服务有限公司、中国电子技术标准化研究院、中国信息安全测评中心、北京奇安信科技有限公司、联想(北京)有限公司、公安部第三研究所、清华大学、中国网络安全审查技术与认证中心、中国科学院软件研究所、中国移动通信集团公司、阿里云计算有限公司、北京天融信科技股份有限公司、中国科学院信息工程研究所、陕西省信息化工程研究院、西北大学、浪潮电子信息产业股份有限公司、北京易华录信息技术股份有限公司、新华三技术有限公司、勤智数码科技股份有限公司、北京数字认证股份有限公司、启明星辰信息技术集团股份有限公司、海信集团有限公司、银川市大数据产业发展服务中心、南京中新赛克科技有限责任公司、北京微步在线科技有限公司、上海观安信息技术有限公司、华为技术有限公司、三六零科技股份有限公司、中电长城网际系统应用有限公司。

本标准主要起草人:朱红儒、刘贤刚、胡影、贾雪飞、白晓媛、叶晓俊、李克鹏、潘亮、薛勇、谢安明、梅婧婷、金涛、叶润国、孙明亮、张宇光、徐羽佳、杜跃进、陈彩芳、柯妍、张玉东、徐雨晴、张世长、宋玲妮、闵京华、郑新华、苗光胜、刘玉岭、潘正泰、张锐卿、任卫红、任兰芳、蔡晓丹、常玲、赵蓓、张大江、唐海龙、孙晓军、李正、孙骞、赵江、马红霞、鲁晋、王川、杜青峰、薛坤、尤其、王伟、张屹、何军、张兴。

# 信息安全技术 数据安全能力成熟度模型

## 1 范围

本标准给出了组织数据安全能力的成熟度模型架构,规定了数据采集安全、数据传输安全、数据存储安全、数据处理安全、数据交换安全、数据销毁安全、通用安全的成熟度等级要求。

本标准适用于对组织数据安全能力进行评估,也可作为组织开展数据安全能力建设的依据。

## 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 25069—2010 信息安全技术 术语

GB/T 29246—2017 信息技术 安全技术信息安全管理 概述和词汇

## 3 术语和定义

GB/T 25069—2010 和 GB/T 29246—2017 界定的以及下列术语和定义适用于本文件。

### 3.1

#### **数据安全 data security**

通过管理和技术措施,确保数据有效保护和合规使用的状态。

### 3.2

#### **保密性 confidentiality**

使信息不泄漏给未授权的个人、实体、进程,或不被其利用的特性。

[GB/T 25069—2010,定义 2.1.1]

### 3.3

#### **完整性 integrity**

准确和完备的特性。

[GB/T 29246—2017,定义 2.40]

### 3.4

#### **可用性 availability**

已授权实体一旦需要就可访问和使用的数据和资源的特性。

[GB/T 25069—2010,定义 2.1.20]

### 3.5

#### **数据安全能力 data security capability**

组织在组织建设、制度流程、技术工具以及人员能力等方面对数据的安全保障。

### 3.6

#### **能力成熟度 capability maturity**

对一个组织有条理的持续改进能力以及实现特定过程的连续性、可持续性、有效性和可信度的