



# 中华人民共和国国家标准

GB/T 30270—2024/ISO/IEC 18045:2022

代替 GB/T 30270—2013

## 网络安全技术 信息技术安全评估方法

Cybersecurity technology—Methodology for IT security evaluation

(ISO/IEC 18045:2022, Information security, cybersecurity and privacy protection—  
Evaluation criteria for IT security—Methodology for IT security evaluation, IDT)

2024-04-25 发布

2024-11-01 实施

国家市场监督管理总局  
国家标准化管理委员会 发布

## 目 次

前言 .....	IX
引言 .....	X
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	2
4 缩略语 .....	4
5 行文方式 .....	5
6 动词用法 .....	5
7 总体评估指南 .....	5
8 ISO/IEC 15408 和本文件结构间的关系 .....	6
9 评估过程与相关任务 .....	6
9.1 概述 .....	6
9.2 评估过程概述 .....	7
9.2.1 目的 .....	7
9.2.2 角色职责 .....	7
9.2.3 角色关系 .....	7
9.2.4 一般评估模型 .....	7
9.2.5 评估者裁定 .....	8
9.3 评估输入任务 .....	9
9.3.1 目的 .....	9
9.3.2 应用注释 .....	9
9.3.3 评估证据子任务的管理 .....	9
9.4 评估子活动 .....	10
9.5 评估输出任务 .....	10
9.5.1 目的 .....	10
9.5.2 评估输出管理 .....	10
9.5.3 应用注释 .....	10
9.5.4 编写 OR 子任务 .....	10
9.5.5 编写 ETR 子任务 .....	11
10 APE 类:PP 评估 .....	18
10.1 概述 .....	18
10.2 已认证 PP 评估结果的复用 .....	18
10.3 PP 引言(APE_INT) .....	18
10.3.1 评估子活动(APE_INT.1) .....	18
10.4 符合性声明(APE_CCL) .....	19
10.4.1 评估子活动(APE_CCL.1) .....	19

10.5	安全问题定义(APE_SPD)	27
10.5.1	评估子活动(APE_SPD.1)	27
10.6	安全目的(APE_OBJ)	28
10.6.1	评估子活动(APE_OBJ.1)	28
10.6.2	评估子活动(APE_OBJ.2)	29
10.7	扩展组件定义(APE_ECD)	31
10.7.1	评估子活动(APE_ECD.1)	31
10.8	安全要求(APE_REQ)	34
10.8.1	评估子活动(APE_REQ.1)	34
10.8.2	评估子活动(APE_REQ.2)	38
11	ACE类:PP配置评估	42
11.1	概述	42
11.2	PP-模块引言(ACE_INT)	43
11.2.1	评估子活动(ACE_INT.1)	43
11.3	PP-模块符合性声明(ACE_CCL)	45
11.3.1	子活动评估(ACE_CCL.1)	45
11.4	PP-模块安全问题定义(ACE_SPD)	48
11.4.1	评估子活动(ACE_SPD.1)	48
11.5	PP-模块安全目的(ACE_OBJ)	49
11.5.1	评估子活动(ACE_OBJ.1)	49
11.5.2	评估子活动(ACE_OBJ.2)	50
11.6	PP-模块扩展组件定义(ACE_ECD)	52
11.6.1	评估子活动(ACE_ECD.1)	52
11.7	PP-模块安全要求(ACE_REQ)	55
11.7.1	评估子活动(ACE_REQ.1)	55
11.7.2	评估子活动(ACE_REQ.2)	59
11.8	PP-模块的一致性(ACE_MCO)	63
11.8.1	评估子活动(ACE_MCO.1)	63
11.9	PP-配置的一致性(ACE_CCO)	66
11.9.1	评估子活动(ACE_CCO.1)	66
12	ASE类:安全目标评估	73
12.1	概述	73
12.2	应用注释	73
12.2.1	重用已认证PP的评估结果	73
12.3	ST引言(ASE_INT)	73
12.3.1	评估子活动(ASE_INT.1)	73
12.4	符合性声明(ASE_CCL)	76
12.4.1	评估子活动(ASE_CCL.1)	76
12.5	安全问题定义(ASE_SPD)	86
12.5.1	评估子活动(ASE_SPD.1)	86
12.6	安全目的(ASE_OBJ)	87
12.6.1	评估子活动(ASE_OBJ.1)	87

12.6.2	评估子活动(ASE_OBJ.2)	88
12.7	扩展组件定义(ASE_ECD)	90
12.7.1	评估子活动(ASE_ECD.1)	90
12.8	安全要求(ASE_REQ)	93
12.8.1	评估子活动(ASE_REQ.1)	93
12.8.2	评估子活动(ASE_REQ.2)	97
12.9	TOE 概要规范(ASE_TSS)	102
12.9.1	评估子活动(ASE_TSS.1)	102
12.9.2	评估子活动(ASE_TSS.2)	102
12.10	复合产品安全目标一致性(ASE_COMP)	103
12.10.1	概述	103
12.10.2	评估子活动(ASE_COMP.1)	104
13	ADV 类:开发	107
13.1	概述	107
13.2	应用注释	107
13.3	安全架构(ADV_ARC)	108
13.3.1	评估子活动(ADV_ARC.1)	108
13.4	功能规范(ADV_FSP)	111
13.4.1	评估子活动(ADV_FSP.1)	111
13.4.2	评估子活动(ADV_FSP.2)	114
13.4.3	评估子活动(ADV_FSP.3)	117
13.4.4	评估子活动(ADV_FSP.4)	121
13.4.5	评估子活动(ADV_FSP.5)	125
13.4.6	评估子活动(ADV_FSP.6)	130
13.5	实现表示(ADV_IMP)	130
13.5.1	评估子活动(ADV_IMP.1)	130
13.5.2	评估子活动(ADV_IMP.2)	132
13.6	TSF 内部(ADV_INT)	134
13.6.1	评估子活动(ADV_INT.1)	134
13.6.2	评估子活动(ADV_INT.2)	136
13.6.3	评估子活动(ADV_INT.3)	137
13.7	安全策略模型(ADV_SPM)	139
13.7.1	评估子活动(ADV_SPM.1)	139
13.8	TOE 设计(ADV_TDS)	144
13.8.1	评估子活动(ADV_TDS.1)	144
13.8.2	评估子活动(ADV_TDS.2)	147
13.8.3	评估子活动(ADV_TDS.3)	150
13.8.4	评估子活动(ADV_TDS.4)	157
13.8.5	评估子活动(ADV_TDS.5)	164
13.8.6	评估子活动(ADV_TDS.6)	170
13.9	复合设计符合性(ADV_COMP)	170
13.9.1	概述	170
13.9.2	评估子活动(ADV_COMP.1)	171

14	AGD类:指导性文档	172
14.1	概述	172
14.2	应用注释	173
14.3	操作用户指南(AGD_OPE)	173
14.3.1	评估子活动(AGD_OPE.1)	173
14.4	准备程序(AGD_PRE)	175
14.4.1	评估子活动(AGD_PRE.1)	175
15	ALC类:生命周期支持	177
15.1	概述	177
15.2	CM能力(ALC_CMC)	177
15.2.1	评估子活动(ALC_CMC.1)	177
15.2.2	评估子活动(ALC_CMC.2)	178
15.2.3	评估子活动(ALC_CMC.3)	179
15.2.4	评估子活动(ALC_CMC.4)	182
15.2.5	评估子活动(ALC_CMC.5)	186
15.3	CM范围(ALC_CMS)	192
15.3.1	评估子活动(ALC_CMS.1)	192
15.3.2	评估子活动(ALC_CMS.2)	193
15.3.3	评估子活动(ALC_CMS.3)	193
15.3.4	评估子活动(ALC_CMS.4)	194
15.3.5	评估子活动(ALC_CMS.5)	195
15.4	交付(ALC_DEL)	196
15.4.1	评估子活动(ALC_DEL.1)	196
15.5	开发安全(ALC_DVS)	197
15.5.1	评估子活动(ALC_DVS.1)	197
15.5.2	评估子活动(ALC_DVS.2)	199
15.6	缺陷纠正(ALC_FLR)	201
15.6.1	评估子活动(ALC_FLR.1)	201
15.6.2	评估子活动(ALC_FLR.2)	203
15.6.3	评估子活动(ALC_FLR.3)	206
15.7	生命周期定义(ALC_LCD)	210
15.7.1	评估子活动(ALC_LCD.1)	210
15.7.2	评估子活动(ALC_LCD.2)	211
15.8	TOE开发构件(ALC_TDA)	212
15.8.1	评估子活动(ALC_TDA.1)	212
15.8.2	评估子活动(ALC_TDA.2)	215
15.8.3	评估子活动(ALC_TDA.3)	218
15.9	工具和技术(ALC_TAT)	221
15.9.1	评估子活动(ALC_TAT.1)	221
15.9.2	评估子活动(ALC_TAT.2)	223
15.9.3	评估子活动(ALC_TAT.3)	225
15.10	复合部分集成及交付程序一致性核查(ALC_COMP)	227

15.10.1	概述	227
15.10.2	评估子活动(ALC_COMP.1)	227
16	ATE类:测试	229
16.1	概述	229
16.2	应用注释	229
16.2.1	了解 TOE 的预期行为	230
16.2.2	验证功能预期行为的测试与替代方法	230
16.2.3	验证测试的充分性	230
16.3	覆盖(ATE_COV)	231
16.3.1	评估子活动(ATE_COV.1)	231
16.3.2	评估子活动(ATE_COV.2)	231
16.3.3	评估子活动(ATE_COV.3)	232
16.4	深度(ATE_DPT)	234
16.4.1	评估子活动(ATE_DPT.1)	234
16.4.2	评估子活动(ATE_DPT.2)	236
16.4.3	评估子活动(ATE_DPT.3)	238
16.4.4	评估子活动(ATE_DPT.4)	240
16.5	功能测试(ATE_FUN)	241
16.5.1	评估子活动(ATE_FUN.1)	241
16.5.2	评估子活动(ATE_FUN.2)	243
16.6	独立测试(ATE_IND)	246
16.6.1	评估子活动(ATE_IND.1)	246
16.6.2	评估子活动(ATE_IND.2)	249
16.6.3	评估子活动(ATE_IND.3)	253
16.7	复合功能测试(ATE_COMP)	253
16.7.1	概述	253
16.7.2	评估子活动(ATE_COMP.1)	253
17	AVA类:脆弱性评定	254
17.1	概述	254
17.2	脆弱性分析(AVA_VAN)	254
17.2.1	评估子活动(AVA_VAN.1)	254
17.2.2	评估子活动(AVA_VAN.2)	258
17.2.3	评估子活动(AVA_VAN.3)	263
17.2.4	评估子活动(AVA_VAN.4)	269
17.2.5	评估子活动(AVA_VAN.5)	274
17.3	复合脆弱性评定(AVA_COMP)	280
17.3.1	概述	280
17.3.2	评估子活动(AVA_COMP.1)	280
18	ACO类:组合	282
18.1	概述	282
18.2	应用注释	282
18.3	组合基本原理(ACO_COR)	283

18.3.1 评估子活动(ACO_COR.1)	283
18.4 开发证据(ACO_DEV)	287
18.4.1 评估子活动(ACO_DEV.1)	287
18.4.2 评估子活动(ACO_DEV.2)	288
18.4.3 评估子活动(ACO_DEV.3)	289
18.5 依赖部件的依赖性(ACO_REL)	291
18.5.1 评估子活动(ACO_REL.1)	291
18.5.2 评估子活动(ACO_REL.2)	293
18.6 组合 TOE 测试(ACO_CTT)	294
18.6.1 评估子活动(ACO_CTT.1)	294
18.6.2 评估子活动(ACO_CTT.2)	296
18.7 组合脆弱性分析(ACO_VUL)	299
18.7.1 评估子活动(ACO_VUL.1)	299
18.7.2 评估子活动(ACO_VUL.2)	301
18.7.3 评估子活动(ACO_VUL.3)	304
附录 A (资料性) 总体评估指南	308
A.1 目的	308
A.2 抽样	308
A.3 依赖关系	309
A.3.1 概述	309
A.3.2 活动之间的依赖关系	309
A.3.3 子活动之间的依赖关系	309
A.3.4 行为之间的依赖关系	310
A.4 现场核查	310
A.4.1 概述	310
A.4.2 一般方法	310
A.5 关于核查列表的指南	311
A.5.1 配置管理方面	311
A.5.2 开发安全方面	311
A.5.3 核查列表示例	312
A.6 评估体制责任	313
附录 B (资料性) 脆弱性评定(AVA)	315
B.1 什么是脆弱性分析	315
B.2 评估者实施脆弱性分析	315
B.3 通用脆弱性指南	315
B.3.1 旁路	316
B.3.2 篡改	317
B.3.3 直接攻击	319
B.3.4 监控	319
B.3.5 误用	320
B.4 识别潜在的脆弱性	320
B.4.1 偶遇识别	321

B.4.2 分析识别 .....	321
B.5 使用攻击潜力 .....	323
B.5.1 开发者 .....	323
B.5.2 评估者 .....	323
B.6 计算攻击潜力 .....	324
B.6.1 攻击潜力的应用 .....	324
B.6.2 刻画攻击潜力 .....	324
B.7 直接攻击的计算实例 .....	329
附录 C (资料性) 评估技术和工具 .....	331
C.1 半形式化和形式化方法 .....	331
C.1.1 概述 .....	331
C.1.2 描述风格 .....	331
参考文献 .....	334



## 前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件代替 GB/T 30270—2013《信息技术 安全技术 信息技术安全性评估方法》。本文件与 GB/T 30270—2013 相比，除结构调整和编辑性改动外，主要技术变化如下：

- 删除了“概述”部分(见 2013 年版的第 5 章)；
- 更改了“文档约定”(见第 5 章、第 6 章、第 7 章、第 8 章,2013 年版的第 6 章)；
- 更改了“通用评估任务”(见第 9 章,2013 年版的第 7 章)；
- 更改了“保护轮廓评估”(见第 10 章,2013 年版的第 8 章)；
- 更改了“ASE 类：安全目标评估”(见第 12 章,2013 年版的第 9 章)；
- 更改了“缺陷纠正子活动”(见 15.6,2013 年版的第 14 章)；
- 删除了“EAL1 评估”“EAL2 评估”“EAL3 评估”和“EAL4 评估”(见 2013 年版的第 10 章、第 11 章、第 12 章和第 13 章)；
- 增加了“ACE 类：PP-配置评估”“ADV 类：开发”“AGD 类：指导性文档”“ALC 类：生命周期支持”“ATE 类：测试”“AVA 类：脆弱性评估”“ACO 类：组合”(见第 11 章、第 13 章、第 14 章、第 15 章、第 16 章、第 17 章、第 18 章)。

本文件等同采用 ISO/IEC 18045:2022《信息安全 网络安全和隐私保护 信息技术安全评估准则 信息技术安全评估方法》。

本文件做了下列最小限度的编辑性改动：

- 为与现有标准协调，将标准名称改为《网络安全技术 信息技术安全评估方法》；
- 为便于使用，在缩略语章节增加了正文中出现的缩略语。

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专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国信息安全测评中心、清华大学、吉林信息安全测评中心、中国网络安全审查技术与认证中心、中国电子科技集团公司第十五研究所、中国合格评定国家认可中心、中国电子技术标准化研究院、中国科学院信息工程研究所、北京市政务信息安全保障中心、华为技术有限公司、北京天融信网络安全技术有限公司、成都卫士通信息安全技术有限公司、中科信息安全共性技术国家工程研究中心有限公司、山东省标准化研究院、陕西省网络与信息安全测评中心、中国汽车工程研究院股份有限公司、浪潮电子信息产业股份有限公司、新华三技术有限公司、北京蓝象标准咨询服务有限公司。

本文件主要起草人：杨永生、毕海英、张宝峰、石竝松、叶晓俊、高金萍、邓辉、王宇航、王亚楠、贾炜、李凤娟、许源、谢仕华、郭昊、刘占丰、张斌、王峰、董晶晶、王鸿娟、牛兴荣、李洪、上官晓丽、朱雪峰、牡丹、刘玉岭、朱克雷、贺海、姚俊宁、王龔、谭儒、王晓楠、雷晓锋、王雁、胡建勋、闻明、刘金琳、李俊、张衡、伊鹏达、宋桂香、刘昱函、朱瑞瑾、骆扬、毛军捷、孙亚飞、庞博、熊琦、饶华一、王蓓蓓、李贺鑫、黄小莉、李静、杨静、万晓兰、乔华阳。

本文件及其所代替文件的历次版本发布情况为：

- 2013 年首次发布为 GB/T 30270—2013；
- 本次为第一次修订。

## 引 言

本文件的目标读者主要是采用 ISO/IEC 15408 的评估者和确认评估者行为的认证者,其次是评估发起者、开发者和保护轮廓、PP-模块、PP-配置、安全目标的作者,以及其他对 IT 安全感兴趣的团体。

本文件并不能解决所有有关 IT 安全评估的问题,有些问题还需要进一步的解释。这些解释将由各评估体制决定如何处理,即便它们要遵从多方互认协议。由各评估体制处理的评估方法相关活动列表见附录 A。本文件旨在与 ISO/IEC 15408 结合使用。

# 网络安全技术

## 信息技术安全评估方法

### 1 范围

本文件描述了在依据 ISO/IEC 15408 标准中所定义的准则和评估证据进行评估时,要求评估者执行的最小行为集。

本文件适用于依据 ISO/IEC 15408 进行的评估活动。

### 2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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 18336.1—2024 网络安全技术 信息技术安全评估准则 第 1 部分:简介和一般模型 (ISO/IEC 15408-1:2022, IDT)

GB/T 18336.2—2024 网络安全技术 信息技术安全评估准则 第 2 部分:安全功能组件 (ISO/IEC 15408-2:2022, IDT)

GB/T 18336.3—2024 网络安全技术 信息技术安全评估准则 第 3 部分:安全保障组件 (ISO/IEC 15408-3:2022, IDT)

GB/T 18336.5—2024 网络安全技术 信息技术安全评估准则 第 5 部分:预定义的安全要求包 (ISO/IEC 15408-5:2022, IDT)

ISO/IEC 15408-1 信息安全、网络安全和隐私保护 信息技术安全评估准则 第 1 部分:简介和一般模型 (Information security, cybersecurity and privacy protection—Evaluation criteria for IT security—Part 1: Introduction and general model)

注: GB/T 18336.1—2024 网络安全技术 信息技术安全评估准则 第 1 部分:简介和一般模型 (ISO/IEC 15408-1:2022, IDT)

ISO/IEC 15408-2 信息安全、网络安全和隐私保护 信息技术安全评估准则 第 2 部分:安全功能组件 (Information security, cybersecurity and privacy protection—Evaluation criteria for IT security—Part 2: Security functional components)

注: GB/T 18336.2—2024 网络安全技术 信息技术安全评估准则 第 2 部分:安全功能组件 (ISO/IEC 15408-2:2022, IDT)

ISO/IEC 15408-3 信息安全、网络安全和隐私保护 信息技术安全评估准则 第 3 部分:安全保障组件 (Information security, cybersecurity and privacy protection—Evaluation criteria for IT security—Part 3: Security assurance components)

注: GB/T 18336.3—2024 网络安全技术 信息技术安全评估准则 第 3 部分:安全保障组件 (ISO/IEC 15408-3:2022, IDT)

ISO/IEC 15408-4 信息安全、网络安全和隐私保护 信息技术安全评估准则 第 4 部分:评估方法和活动的规范框架 (Information security, cybersecurity and privacy protection—Evaluation criteria for IT security—Part 4: Framework for specification of evaluation methods and activities)

注: GB/T 18336.4—2024 网络安全技术 信息技术安全评估准则 第 4 部分:评估方法和活动的规范框架