



# 中华人民共和国国家标准化指导性技术文件

GB/Z 29830.2—2013/ISO/IEC TR 15443-2:2005

GB/Z 29830.2—2013/ISO/IEC TR 15443-2:2005

## 信息技术 安全技术 信息技术安全保障框架 第2部分:保障方法

Information technology—Security technology—A framework for IT security assurance—Part 2: Assurance methods

[ISO/IEC TR 15443-2:2005, IDT]

中华人民共和国  
国家标准化指导性技术文件  
信息技术 安全技术  
信息技术安全保障框架  
第2部分:保障方法

GB/Z 29830.2—2013/ISO/IEC TR 15443-2:2005

\*

中国标准出版社出版发行  
北京市朝阳区和平里西街甲2号(100029)  
北京市西城区三里河北街16号(100045)  
网址 www.spc.net.cn  
总编室:(010)64275323 发行中心:(010)51780235  
读者服务部:(010)68523946  
中国标准出版社秦皇岛印刷厂印刷  
各地新华书店经销

\*

开本 880×1230 1/16 印张 3.25 字数 84 千字  
2014年4月第一版 2014年4月第一次印刷

\*

书号: 155066·1-48741 定价 45.00 元

如有印装差错 由本社发行中心调换  
版权专有 侵权必究  
举报电话:(010)68510107



GB/Z 29830.2-2013

2013-11-12 发布

2014-02-01 实施

中华人民共和国国家质量监督检验检疫总局  
中国国家标准化管理委员会 发布

## 目 次

前言 .....	III
引言 .....	IV
1 范围 .....	1
1.1 意图 .....	1
1.2 适用领域 .....	1
1.3 限制 .....	1
2 规范性引用文件 .....	2
3 术语、定义和缩略语 .....	3
4 方法概述和表达 .....	3
5 保障的生存周期阶段与图示符号 .....	3
5.1 保障途径与图示符号 .....	4
5.2 实用性与符号表示 .....	4
5.3 安全相关性与符号表示 .....	4
5.4 概览表 .....	4
5.5 表达方法学 .....	6
6 保障方法 .....	6
6.1 ISO/IEC 15408 信息技术安全评估准则	6
6.2 TCSEC 可信计算机系统评估准则	7
6.3 ITSEC/ITSEM 信息技术安全评估准则和方法学	8
6.4 CTCPEC 加拿大可信产品评估准则	9
6.5 KISEC/KISEM 韩国信息安全评估准则和方法学	10
6.6 RAMP 维护阶段的评定	11
6.7 ERM 评估评定的维护(一般性的)	12
6.8 TTAP 可信技术评价程序	13
6.9 TPEP 可信产品评估程序	13
6.10 Rational 统一过程®(RUP®)	14
6.11 ISO/IEC 15288 系统生存周期过程	15
6.12 ISO/IEC 12207 软件生存周期过程	16
6.13 V-模型	17
6.14 ISO/IEC 14598 软件产品评价	18
6.15 X/Open 基线安全服务	19
6.16 SCT 严格符合性测试	20
6.17 ISO/IEC 21827 系统安全工程 能力成熟度模型(SSE-CMM®)	21
6.18 TCMM 可信任能力成熟度模型	22
6.19 CMMI 集成化能力成熟度模型®	23
6.20 ISO/IEC 15504 软件过程评估	24

6.21 CMM 能力成熟度模型®(针对软件) ..... 25

6.22 SE-CMM® 系统工程能力成熟度模型® ..... 26

6.23 TSDM 可信任软件开发方法 ..... 26

6.24 SDoC 提供方符合性声明 ..... 27

6.25 SA-CMM® 软件需求能力成熟度模型® ..... 28

6.26 ISO 9000 系列 质量管理 ..... 29

6.27 ISO 13407 以人为中心的设计(HCD) ..... 30

6.28 开发者良源(一般情况) ..... 31

6.29 ISO/IEC 17025 鉴定保障..... 31

6.30 ISO/IEC 13335 信息和通信技术安全管理(MICTS) ..... 32

6.31 BS 7799-2 信息安全管理系统 规格说明与使用指导® ..... 33

6.32 ISO/IEC 17799 信息安全管理实践指南® ..... 34

6.33 FR 缺陷补救(一般性) ..... 35

6.34 IT 基线保护指南® ..... 35

6.35 渗透测试® ..... 36

6.36 人员认证(与安全无关) ..... 37

6.37 人员认证(与安全有关)® ..... 38

参考文献 ..... 40

图 1 ISO/IEC 14598 评价过程的流程 ..... 19

表 1 框架中的保障方法—图示符号 ..... 4

表 2 框架中保障方法—概览 ..... 5

表 3 SA-CMM®关键过程领域 ..... 28

表 4 鉴定过程 ..... 32

[47] A Trusted Software Development Methodology J. Watson and E. Amoroso, in Proc. 13th Natl. Computer Security Conf, Oct. 1990, pp. 717-727.

[48] Insider Threat Mitigation Report in Final Report of the Insider Threat Integrated Process Team, IPT April 24, 2000. Insider Threat Integrated Process Team, Department of Defense, USA.

[49] State of the Practice of Intrusion Detection Technologies CMU/SEI-99-TR-028 ESC-TR-99-028, January 2000. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890, USA.

Note: The document may be available as <http://www.sei.cmu.edu/pub/documents/99.reports/pdf/99tr028.pdf>

[50] Korea Information Security Evaluation Criteria(KISEC) Ministry of Information and Communication, Republic of Korea, February 1998.

[51] Korea Information Security Evaluation Methodology(KISEM) Ministry of Information and Communication, Republic of Korea, November 1998.

[52] Philippe Kruchten, The Rational Unified Process—An Introduction Addison-Wesley-Longman, Reading, MA, USA

[53] BS 7799-2:2002 Information security management systems—Specification with guidance for use BSI(British Standards Institution), Customer Services, 389 Chiswick High Road, London W4 4AL, United Kingdom