ICS 35.040

L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

中华人民共和国国家标准

GB/T 18336.3-2015/ISO/IEC 15408-3: 2008

Replace GB/T 18336.3-2008

Information technology—Security techniques—Evaluation criteria for IT security—Part 3: Security assurance components

信息技术 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: 2008, IDT)

Issued on May 15, 2015 Implemented on January 01, 2016

Issued by General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China

Standardization Administration of the People's Republic of China

Contents

Foreword

GB/T 18336 “Information technology--Security techniques--Evaluation criteria for IT security” includes the following 3 parts:

— part 1: Introduction and general model;

— part 2: Security functional components;

— part 3: Security assurance components.

This part is part 3 of GB/T 18336.

This part is drafted in accordance with specifications in GB/T1.1-2009.

This part will replace GB/T 18336.3-2008 “Information technology--Security techniques--Evaluation criteria for IT security part 3: Security assurance components”.

The main differences between this part and GB/T 18336.3-2008 are as follows:

— “assurance” is replaced by “guarantee”;
— "6 Security assurance requirements" is replaced by "6 Security assurance components";
— "6.3 Protection profile and security target evaluation criteria class structure "," 6.4 Usage of terms in this part", "6.5 Assurance classification" and “6.6 General situation of assurance classes and families” are removed;
— "6.1.5 EAL structure" is reedited as "6.2 Evaluation assurance levels structure" in this part;
— “6.3 Combination assurance package structure” is added;
— "7 Protection profile and security target evaluation criteria " and "11 assurance classes , families and components" are removed;
— "8 Combination assurance package" is added;
— "8.1 TOE description" is removed;
— "9.2 Conformance declaration " is added;
— "8.2 Security environment" and "8.6 Clearly stated IT security requirements" are amended as "9.3 Security problem definition" and "9.5 Extended components

definition";

— "9.1 TOE description " and "9.5 PP declaration" are removed;

— "10.2 Conformance declaration " is added;

— "9.2 Security environment" and “9.7 Clearly stated IT security requirements" are amended as “10.3 Security problem definition" and "10.5 Extended components definition";

— "High level design (ADV_HLD)" , "Low level design(ADV_LLD)" and " Representing corresponding relationship(ADV_RCR) " in "ADV class: development" are removed;

— " Security architecture (ADV_ARC)" and "TOE design (ADV_TDS)" are added in "ADV class: development";

— "Administrator guidelines (AGD_ADM)" and " User guidelines (AGD_USR)" of AGD class are amended as " Operator guidelines(AGD_OPE)" and "Preparation (AGD_PRE)";

— " CM capability (ACM_CAP)" and "CM scope (ACM_SCP)" in ACM class as well as "delivery (ADO_DEL)" in ADO class are combined into ALC class;

— "CM automation (ACM_AUT)" in "ACM class: configuration management" is removed;

— "Installation, generation and starting (ADO_IGS) in "ADO class: delivery and operation" is removed;

— "Test cover (ATE_COV)" is amended as "Cover (ATE_COV)" while "Test depth (ATE_DPT)" is amended as" Depth (ATE_DPT);

— " Concealed channel analysis (AVA_CCA)", "Misusing (AVA_MSU)" and "TOE strength of function (AVA_SOF)" in "AVA class: vulnerability evaluation" are removed;

— "Vulnerability analysis(AVA_VLA)" is amended as "Vulnerability analysis(AVA_VAN)";

— "16 ACO class: combination" is added;

— "Annex A development (ADV)", "Annex B combination (ACO)" and "Annex D cross-reference between PP and assurance components" and "Annex F Cross-reference between CAP and assurance components" are added;

— “Annex A Cross-reference of dependency relationship of assurance components” is amended as “Annex C Cross-reference of dependency relationship of assurance

components”. “Annex B Cross-reference between EAL and assurance components” is amended as “Annex E Cross-reference between EAL and assurance components” .

This part is a translation copy and identical to the international standard ISO/IEC 15408-3:2008 “Information technology--Security techniques--Evaluation criteria for IT security part 3: Security assurance components”.

The consistent domestic documents corresponding to normative international references in this part are as follows:

--GB/T 18336.1 Information technology--Security techniques--Evaluation criteria for IT security part1: Introduction and general mode (GB/T 18336.1-2015, ISO/IEC 15408--1: 2009, IDT)

--GB/T 18336.2 Information technology--Security techniques--Evaluation criteria for IT security part 2: Security functional components (GB/T 18336.2-2015, ISO/IEC 15408--2: 2008, IDT)

This part is proposed and under jurisdiction of China Information Security Standardization Technical Committee (SAC/TC 260).

The main drafting units of this standard include: China Information Technology Security Evaluation Center, Information Technology Security Test and Evaluation Center, The Third Research Institute of Ministry of Public Security.

The main drafters of this part include: Zhang Chongbin, Guo Ying, Shi Hongsong, Bi Haiying, Zhang Baofeng, Gao Jinping, Wang Feng, Yang Yongsheng, Li Guojun, Dong Jingjing, Xie Di, Wang Hongxian, Zhang Yi, Gu Jian, Qiu Zihua, Song Haohao, Chen Yan, Yang Yuanyuan, Xu Yuan, Rao Huayi, Wu Yushu, Mao Junjie.

The previous editions replaced by this part are as follows:

--GB/T 18336.3-2001;

--GB/T 18336.3-2008.

INTRODUCTION

Security assurance components, as defined in this part, are the basis for the security assurance requirements expressed in a Protection Profile (PP) or a Security Target (ST).

These requirements establish a standard way of expressing the assurance requirements for TOEs. This part catalogues the set of assurance components, families and classes. This part also defines evaluation criteria for PPs and STs and presents evaluation assurance levels that define the predefined ISO/IEC 15408 scale for rating assurance for TOEs, which is called the Evaluation Assurance Levels (EALs).

The audience for this part includes consumers, developers, and evaluators of secure IT products. ISO/IEC 15408-1 provides additional information on the target audience of ISO/IEC 15408, and on the use of IEC 15408 by the groups that comprise the target audience. These groups may use this part as follows:

a) Consumers, who use this part when selecting components to express assurance requirements to satisfy the security objectives expressed in a PP or ST, determining required levels of security assurance of the TOE.

b) Developers, who respond to actual or perceived consumer security requirements in constructing a TOE, reference this part when interpreting statements of assurance requirements and determining assurance approaches of TOEs.

c) Evaluators, who use the assurance requirements defined in this part as a mandatory statement of evaluation criteria when determining the assurance of TOEs and when evaluating PPs and STs.

Information technology—Security techniques—Evaluation criteria for IT security—Part 3: Security assurance components

1 Scope

This part of GB/T 18336 defines the assurance requirements. It includes the evaluation assurance levels (EALs) that define a scale for measuring assurance for component TOEs, the composed assurance packages (CAPs) that define a scale for measuring assurance for composed TOEs, the individual assurance components from which the assurance levels and packages are composed, and the criteria for evaluation of PPs and STs.

2 Normative references

The articles contained in the following documents have become this document when they are quoted herein. For the dated documents so quoted, all the modifications (Including all corrections) or revisions made thereafter shall be applicable to this document.

ISO/IEC 15408-1, Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model

ISO/IEC 15408-2, Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components

3 Terms and definitions

For the purposes of this document, the terms, definitions, symbols and abbreviated terms given in ISO/IEC 15408-1 apply.

4 Overview

4.1 Organisation of this part

Clause 5 describes the paradigm used in the security assurance requirements of this part.

Clause 6 describes the presentation structure of the assurance classes, families, components, evaluation assurance levels along with their relationships, and the structure of the composed assurance packages. It also characterises the assurance classes and families found in Clauses 9 through 16.

Clause 7 provides detailed definitions of the EALs.

Clause 8 provides detailed definitions of the CAPs.

Clauses 9 through 16 provide the detailed definitions of this part assurance classes.

Annex A provides further explanations and examples of the concepts behind the Development class.

Annex B provides an explanation of the concepts behind composed TOE evaluations and the Composition class.

Annex C provides a summary of the dependencies between the assurance components.

Annex D provides a cross reference between PPs and the families and components of the APE class.

Annex E provides a cross reference between the EALs and the assurance components.

Annex F provides a cross reference between the CAPs and the assurance components.

5 Assurance paradigm

The purpose of this Clause is to document the philosophy that underpins ISO/IEC 15408 approach to assurance. An understanding of this Clause will permit the reader to understand the rationale behind this part assurance requirements.

5.1 ISO/IEC 15408 philosophy

ISO/IEC 15408 philosophy is that the threats to security and organisational security policy commitments should be clearly articulated and the proposed security measures be demonstrably sufficient for their intended purpose.

Furthermore, measures should be adopted that reduce the likelihood of vulnerabilities, the

北京文心雕语翻译有限公司
Beijing Lancarver Translation Inc.

完整版本请在线下单/Order Checks Online for Full version

联系我们/or Contact:

TEL: 400-678-1309

QQ: 19315219 | Skype: Lancarver

Email：info@lancarver.com

http://www.lancarver.com

线下付款方式：

I. 对公账户：

单位名称：北京文心雕语翻译有限公司

开 户 行：中国工商银行北京学清路支行

账　　号：0200 1486 0900 0006 131

II. 支付宝账户：info@lancarver.com

III. Paypal: info@lancarver.com

注: 付款成功后，请预留电邮，完整版本将在一个工作日内通过电子 PDF 或 Word 形式发送至您的预留邮箱，如需索取发票，下单成功后的三个工作日内安排开具并寄出，预祝合作愉快！

NOTE All documents on the store are in electronic Adobe Acrobat PDF format, there is not sell or ship documents in hard copy. Mail the order and payment information to info@lancarver.com , you will shortly receive an e-mail confirming your order.