

ICS 35.030
CCS L 80



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 18336.4-2024

Replacing GB/T 18336.3-2015

**Cybersecurity technology - Evaluation criteria for IT security -
Part 4: Framework for specification of evaluation methods and
activities**

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
(English Translation)

Issued on: April 25, 2024

Implemented on: November 1, 2024

**Issued by: State Administration for Market Regulation, China National
Standardization Administration**

Table of Contents

Preface
Introduction
1 Scope
2 Normative references
3 Terms and Definitions
4 Evaluation methods and general model of evaluation activities
4.1 Concepts and Models
4.2 Using derivative methods to develop assessment methods and assessment activities
4.3 Verb usage in descriptions of assessment methods and assessment activities
4.4 Conventions for describing evaluation methods and evaluation activities
5 Structure of the evaluation method
5.1 Overview
5.2 Specification of evaluation methods
6 Structure of the Assessment Activity 10
6.1 Overview
6.2 Description of the assessment activities
Appendix NA (Informative) Abbreviations
Reference

Foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for standardization work Part 1: Structure and drafting rules for standardization documents" Drafting:

This document is part 4 of GB/T 18336 "Cybersecurity Technology Information Technology Security Assessment Criteria": GB/T 18336 has been Post the following parts:

- Part 1: Introduction and general model;
- Part 2: Safety functional components;
- Part 3: Safety assurance components;
- Part 4: Normative framework for assessment methods and activities;
- Part 5: Predefined security requirements package:

This document and GB/T 18336.3-2024 "Cybersecurity Technology Information Technology Security Assessment Criteria Part 3: Security Assurance Group GB/T 18336.5-2024 "Information Security Technology Network Technology Security Assessment Criteria Part 5: Predefined Security Requirements Package" Replace GB/T 18336.3-2015 "Information Technology Security Technology Information Technology Security Assessment Criteria Part 3: Security Assurance" Components:

This document partially replaces GB/T 18336.3-2015 "Network Technology Security Technology Information Technology Security Assessment Criteria Part 3" Compared with GB/T 18336.3-2015, in addition to structural adjustments and editorial changes, the main technical changes are as follows:

- Added the general model of evaluation methods and evaluation activities (see Chapter 4);
- Deleted the protection model (see Chapter 5 of GB/T 18336.3-2015 edition);
- Deleted the safety assurance component (see Chapter 6 of GB/T 18336.3-2015 edition);
- Added the structure of the evaluation method (see Chapter 5);
- Added the structure of evaluation activities (see Chapter 6);
- Deleted the assessment assurance level (see Chapter 7 of GB/T 18336.3-2015 edition);
- Deleted the combined guarantee package (see Chapter 8 of GB/T 18336.3-2015 edition);
- Deleted APE category: Assurance profile evaluation (see Chapter 9 of GB/T 18336.3-2015 edition);
- Deleted ASE category: Safety objective assessment (see Chapter 10 of GB/T 18336.3-2015 edition);
- Deleted ADV category: Development (see Chapter 11 of GB/T 18336.3-2015 edition);
- Deleted AGD category: Guidance document (see Chapter 12 of GB/T 18336.3-2015 edition);
- Deleted the ALC class: Lifecycle support (see Chapter 13 of GB/T 18336.3-2015 edition);
- Deleted ATE category: Test (see Chapter 14 of GB/T 18336.3-2015 edition);
- Deleted the AVA category: Vulnerability assessment (see Chapter 15 of GB/T 18336.3-2015 edition);
- Deleted ACO category: combination (see Chapter 16 of GB/T 18336.3-2015 edition);

This document is equivalent to ISO/IEC 15408-4:2022 "Information security, network

security and privacy protection information technology security assessment standards" Part 4: Normative framework for assessment methods and activities:

The following minimal editorial changes were made to this document:

--- In order to coordinate with the existing standards, the name of the standard will be changed to "Cybersecurity Technology Information Technology Security Assessment Criteria Part 4: Assessment Normative framework for assessment methods and activities;

--- Add informative Appendix NA "Abbreviations":

Introduction

The readers of this document are mainly assessors who adopt GB/T 18336-2024 and certifiers who confirm the assessors' behavior, as well as Assessment sponsors, developers, PP/ST authors and other groups interested in IT security:

GB/T 18336 is planned to consist of five parts:

--- Part 1: Introduction and general model: This aims to provide an overall overview of GB/T 18336 and define the basic principles of information technology security assessment:

The paper introduces general concepts and principles and gives a general model for evaluation:

--- Part 2: Safety functional components: Aims to establish a set of standardized templates for functional components that can be used to describe safety functional requirements:

These functional components are structured in the form of classes and families, and specific functions are constructed through component selection, refinement, and cutting:

safety functional requirements:

--- Part 3: Security assurance components: Aims to establish a set of standardized templates for security assurance components that can be used to describe security assurance requirements:

These security assurance components are structured in classes and families, defining the criteria for evaluation of PP, ST, and TOE:

Then, specific security requirements are constructed through component selection, refinement, and tailoring:

--- Part 4: Normative framework for evaluation methods and activities: Aims to provide a standardized framework for normative evaluation methods and activities:

These assessment methods and activities are included in the PP, ST and any supporting documents for assessors to use based on the evaluation work is carried out based on the models described in other parts of GB/T 18336:

--- Part 5: Predefined security requirement packages: Aims to provide security assurance requirements and security functions commonly used by stakeholders Required packages, examples of packages provided include Evaluation Assurance Level (EAL) and Combined Assurance Package (CAP):

GB/T 18336 provides a set of general security functions and safeguard measures for the security assessment of information technology (IT) products:

ISO/IEC 18045 is a standard set by GB/T 18336:

Some of the safeguard requirements provide supporting methods:

This document describes a framework that can be used to derive assessment activities from ISO/IEC 18045 work units and group them into assessment Method (EM): Evaluation activities or evaluation methods may be included in the PP and any supporting documents:

When determining whether a specific assessment method/assessment activity is to be used for a block, package or safety target (ST), ISO/IEC 18045 requires the assessor to when assessing, the assessor follows and reports on the relevant assessment methods/assessment activities: As described in GB/T 18336.1, in some cases, the assessment the authorising body can decide not to approve the use of a particular assessment method/assessment activity: In this case, the assessment authorising body can decide not to approve the use of a particular assessment method/assessment activity:

The assessment method/assessment activities required by ST will be assessed:

This document also allows the definition of assessment activities for extended SARs, in which case the assessment activities are derived from the same criteria as those defined for extended SARs:

If this document refers to the use of SAR in ISO/IEC 18045 or ISO/IEC 15408-3 (such as when defining the rationale for the assessment activity), then in the case of an extended SAR, such reference will also apply to the criteria defined for the extended SAR:

Equivalent behavioral elements and units of work:

For the sake of simplicity, this document specifies how to define assessment methods and assessment activities, but does not itself prescribe the methods or activities of assessment:

Example:

The following notes appearing in other parts of GB/T 18336 and GB/T 30270-2024 describe the provisions of those documents regarding the boldface this document does not use those conventions, but the notes are retained here for consistency with other standards:

Note: This document uses bold and italic fonts in some cases to distinguish terms from the rest of the text:

For layered components, when the requirements are enhanced or modified beyond those of