

ICS 35.030
CCS L 80



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

GB/T 32916-2023

Replacing GB/Z 32916-2016

**Information security techniques - Guidelines for the
assessment of information security controls**

信息安全技术 信息安全控制评估指南

(English Translation)

Issued on: September 7, 2023

Implemented on: April 1, 2024

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

Table of Contents

Preface	
Introduction	
1 Scope	
2 Normative reference documents	
3 Terms and Definitions	
4 Structure of this document	
5 Background	
6 Overview of information security control assessment	
6.1 Assessment process	
6.2 Resources and Capabilities	4
7 Assessment Methods	
7.1 General	
7.2 Process Analysis	
7.3 Check	
7.4 Testing and Validation	
7.5 Sampling	
8 Control Measures Assessment Process	8
8.1 Preparation	
8.2 Planning and evaluation	
8.3 Implementation Assessment	13
8.4 Analyzing and reporting results	14
Appendix A (Informative) Initial Information Collection (Except Information Technology)	
Appendix B (Informative) Technical Security Assessment Practical Guide	
Appendix C (Informative) Cloud Service (Infrastructure as a Service) Technical Assessment Guide	50
Appendix NA (informative) Correspondence between GB/T 22081-2016 and ISO/IEC 27002:2022 control measures	
Reference	

Foreword

This document complies with the provisions of GB/T 1.1-2020 "Standardization Work Guidelines Part 1: Structure and Drafting Rules of Standardization Documents" Drafting.

This document replaces GB/Z 32916-2016 "Information Technology Security Technology Information Security Control Measures Auditor's Guide" and is consistent with GB/Z 32916-Compared with 2016, in addition to structural adjustments and editorial changes, the main technical changes are as follows.

---An introduction to sampling has been added to the evaluation method (see 7.5).

This document is equivalent to ISO/IEC TS27008:2019 "Information Technology Security Technology Information Security Control Assessment Guide", document the type is adjusted from ISO/IEC technical specifications to my country's national standards.

This document has made the following minimal editorial changes.

- a) In order to coordinate with existing standards, the name of the standard is changed to "Information Security Technology Information Security Control Assessment Guide";
- b) Added Appendix NA.

Please note that some content in this document may be subject to patents. The publisher of this document assumes no responsibility for identifying patents.

Introduction

This document supports the information security risk management process given in GB/T 22080-2016, as well as the relevant information security identified Set of control measures.

Information security controls should be applicable, effective and efficient. This document describes how to evaluate information security risks and other objectives.

Evaluate the organization's information security controls to confirm that they are appropriate, effective, and efficient, or to identify the need for changes (improvement opportunities). information the ultimate goal of security controls as a whole is to adequately mitigate what the organization considers to be undesirable issues in a cost-effective and business-consistent manner.

Acceptable and unavoidable information security risks. Based on business mission and objectives, organizational policies and requirements, identified threats and vulnerabilities, operational this document provides the flexibility needed to tailor the necessary assessment to operational considerations, information system and platform dependencies, and organizational risk considerations.

active.

For information security management system audit guidelines, see GB/T 28450-2020, and for information security management system audit and certification agencies See GB/T 25067-2020 for the requirements.

Note: "Information security control measures" and "information security controls" can be used

interchangeably in this document. For the definition of "control", see GB/T 29246-2017.

Information security technology Information Security Control Assessment Guide

1 Scope

This document provides guidance on the implementation and operation of information security controls and the assessment process, including information system control measures.

Technical assessment, which is based on the information security requirements and technical assessment criteria established by the organization.

This document explains how to evaluate information security controls managed by an information security management system specified in ISO/IEC 27001.

Provide guidance.

This document is suitable for organizations of all types and sizes conducting information security assessments and technical compliance checks.

2 Normative reference documents

The contents of the following documents constitute essential provisions of this document through normative references in the text. Among them, the dated quotations for undated referenced documents, only the version corresponding to that date applies to this document; for undated referenced documents, the latest version (including all amendments) applies to this document.

Note: GB/T 29246-2017 Information technology security technology information security management system overview and vocabulary (ISO/IEC 27000:2016, IDT)

3 Terms and definitions

The terms and definitions defined in ISO/IEC 27000 apply to this document.

4 Structure of this document

This document describes the process for evaluating information security controls, including technical assessments.

Chapter 5 provides background information.

Chapter 6 provides an overview of information security control assessment.

Chapter 7 introduces evaluation methods.

Chapter 8 introduces the information security control assessment process.

Appendix A guides initial information collection.

Appendix B guides technical assessment.

Appendix C guides the technical evaluation of cloud services.

Appendix NA gives the correspondence between the control measures in GB/T 22081-2016 and ISO/IEC 27002:2022.

5 Background

Information security controls are the main means of dealing with unacceptable information security risks and keeping them within the acceptable risk level of the organization.

means.