

ICS 35.030
CCS L 80



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

GB/T 43577.1-2023

**Information security technology - Electronic discovery - Part 1:
Overview and concepts**

信息安全技术 电子发现 第1部分：概述和概念
(English Translation)

Issued on: December 28, 2023

Implemented on: July 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 Abbreviations	
5 GB/T 43577 overall structure and overview	
6 Electronic Discovery Overview	
6.1 Background	
6.2 Basic concepts	
6.3 Goals of electronic discovery	
6.4 Basics of electronic discovery	
6.5 Governance and eDiscovery	
6.6 ICT readiness for e-discovery	
6.7 Planning and Budgeting for Electronic Discovery Projects	
7 Electronically retained information (ESI)	
7.1 Background	
7.2 Common types of ESI	
7.3 Common sources of ESI ¹⁰	
7.4 ESI Presentation	
7.5 The non-ESI part of discovery	
8 The electronic discovery process 12	
8.1 Overview	
8.2 ESI identification	
8.3 ESI security	
8.4 ESI Collection	
8.5 ESI processing	
8.6 ESI Review	
8.7 ESI analysis	
8.8 ESI output	
9 Other considerations 15	
9.1 ESI Presentation	

9.2 Chain of custody and provenance 15

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 is Part 1 of GB/T 43577 "Information Security Technology Electronic Discovery": GB/T 43577 has released the following part:

---Part 1: Overview and concepts:

This document is equivalent to ISO/IEC 27050-1:2019 "Information technology electronic discovery - Part 1: Overview and concepts":

This article has made the following minimal editorial changes:

---In order to coordinate with existing standards, the name of the standard is changed to "Information Security Technology Electronic Discovery Part 1: Overview and Concepts"

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

Electronic discovery is often a driver of investigations and evidence acquisition and processing activities (covered in ISO/IEC 27037): In addition, data the sensitivity and criticality of data sometimes require protective measures such as storage security (covered in ISO/IEC 27040) to prevent data security Completely damaged: GB/T 43577 aims to standardize the related concepts, governance and management, processes and activities, and technical preparation of electronic discovery: It is planned to be it consists of the following four parts:

---Part 1: Overview and concepts: The purpose is to describe e-discovery concepts and their processes and to define related terms:

---Part 2: Guidelines for the Governance and Management of Electronic Discovery: The purpose is to provide governance for e-discovery to senior management of an organization and management guidelines:

---Part 3: Practical Guide to Electronic Discovery: The purpose is to put forward requirements and suggestions for various activities in the electronic discovery process:

---Part 4: Technology Ready: The purpose is to provide organizations with technical and process perspectives for planning, preparing, and implementing eDiscovery:

guide:

For more information about ISO/IEC 27050, see Chapter 5:

Information Security Technology Electronic Discovery Part 1: Overview and Concepts

1 Scope

Electronic discovery is the discovery of electronically retained information (ESI) or data by one or more parties involved in an investigation, litigation, or similar proceeding:

process: This document provides an overview of electronic discovery, defines related terms, and describes related concepts, including but not limited to the identification, preservation, and collection of ESI:

Collect, process, review, analyze and produce: This document also identifies other relevant standards (such as ISO/IEC 27037) and their relevance to e-discovery activities relationships and interactions:

This document is intended for non-technical and technical personnel involved in some or all e-discovery activities:

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 29246-2023 Information security technology information security management system overview and vocabulary (ISO/IEC 27000:2018, IDT)

3 Terms and definitions

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

chain of custody Demonstrable possession, movement, handling and location of materials from one point in time to another:

Custodian

A person or entity who has custody, control or possession of electronically retained information (3:8):

Data security compromised databreach the security of protected data is reduced, resulting in accidental or illegal destruction, or illegal destruction during transmission, storage or other processing:

Loss, alteration or unauthorized disclosure or access:

[Source: ISO/IEC 27040:2015,3:7] 3.4 discoverydiscovery the process by which one party obtains information related to a matter that is held by another party or that is not held by either party:

Note 1: Discovery has a wider scope of application than the parties in adversarial disputes:

Note 2: Discovery also refers to the disclosure of the other party's hard copy documents, electronically retained information (3:8) and tangible items:

Note 3: In some jurisdictions, the terms "disclosure" and "discovery" are used interchangeably: