Doc No: LITD 17 (24473)
Draft IS/ISO/IEC 27036-3:2023
December 2023

BUREAU OF INDIAN STANDARDS

DRAFT FOR COMMENTS ONLY

(Not to be reproduced without the permission of BIS or used as an Indian Standard)

मसौदा भारतीय मानक

साइबरसुरक्षा - आपूर्तिकारों से संबंध- भाग 3: हार्डवेयर, सॉफ्टवेयर और सेवा आपूर्ति श्रृंखला सुरक्षा हेतु दिशानिर्देश

(पहला पुनरीक्षण)

.

Draft Indian Standard

Cybersecurity — Supplier Relationships — Part 3: Guidelines for Hardware, Software, and Services Supply Chain Security

(First Revision)

ICS 35.030

Information Systems Security And Privacy Sectional Committee, LITD 17	**Last Date for Comments: 20 Feb 2024**

NATIONAL FOREWORD

(Formal clauses will be added later)

This draft Indian Standard (Part 3) (First Revision) which is identical to ISO/IEC 27036-3:2023 ‘Cybersecurity Supplier relationships Part 3: Guidelines for hardware, software, and services supply chain security' issued by International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) will be adopted by the Bureau of Indian Standards (BIS) on the recommendations of the Information Systems Security And Privacy Sectional Committee, LITD 17 and approval of the Electronics and Information Technology Division Council.

This Indian Standard is published in several parts. The other parts in this series are:

Part 1: Overview and concepts (First Revision)
Part 2 Requirements
Part 4 Guidelines for Security of Cloud Services

The main changes are as follows:
— the structure and content have been aligned with the most recent version of ISO/IEC/IEEE 15288;
— former Annex A has been removed;
— Annex B has been added

The text of ISO/IEC Standard may be approved as suitable for publication as an Indian Standard without deviations. Certain conventions are however not identical to those used in Indian Standards. Attention is particularly drawn to the following:

a) Wherever the words 'International Standard' appears referring to this standard, they should be read as 'Indian Standard'.

b) Comma (,) has been used as a decimal marker while in Indian Standards, the current Practice is to use a point (.) as the decimal marker.

In this adopted standard, reference appears to certain International Standards for which the Indian Standard also exists. The corresponding Indian Standard which is to be substituted in its respective place is listed below along with its degree of equivalence for the edition indicated. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies:

International Standards	**Corresponding Indian Standard**	**Degree of Equivalence**
ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary	IS/ISO/IEC 27000 : 2018 Information technology - Security techniques - information: Security management systems - Overview and vocabulary (First Revision)	Identical with ISO/IEC 27000 : 2018
ISO/IEC 27036-1, Cybersecurity — Supplier relationships — Part 1: Overview and concepts	IS/ISO/IEC 27036-1 : 2021 Cybersecurity Supplier relationships Part 1: Overview and concepts First Revision	Identical with ISO/IEC 27036-1: 2021

Doc No: LITD 17 (24473)
Draft IS/ISO/IEC 27036-3:2023
December 2023

Scope of ISO/IEC 27036-3:2023 is as follows:

"This document provides guidance for product and service acquirers, as well as suppliers of hardware, software and services, regarding:
a) gaining visibility into and managing the information security risks caused by physically dispersed and multi-layered hardware, software, and services supply chains;
b) responding to risks stemming from this physically dispersed and multi-layered hardware, software, and services supply chain that can have an information security impact on the organizations using these products and services;
c) integrating information security processes and practices into the system and software life cycle processes, as described in ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207, while supporting information security controls, as described in ISO/IEC 27002.
This document does not include business continuity management/resiliency issues involved with the hardware, software, and services supply chain. ISO/IEC 27031 addresses information and communication technology readiness for business continuity."

Note: - The technical content of this document has not been enclosed as these are identical with the corresponding ISO/IEC Standard. For details please refer to ISO/IEC 27036-3:2023 or kindly contact.

Head,
Electronics & IT Department
Bureau of Indian Standards
9, B.S. Zafar Marg,
New Delhi-110002
Email: hlitd@bis.gov.in, litd17@bis.gov.in
Tele: 011-23608450