EDC 4 (3136) DTZS
ISO/IEC 27036-2:2022

DRAFT TANZANIA STANDARD

(Draft for comments only)

Cybersecurity – Supplier relationships – part 2: Requirements

TANZANIA BUREAU OF STANDARDS

First Edition 2024

0 National Foreword

This draft Tanzania Standard is being prepared by the Alarm and Electronic Security Systems Technical Committee of the Tanzania Bureau of Standards (TBS), under the supervision of the Electrotechnical Divisional Standards Committee (EDC)

This Tanzania Standard is an adoption of the International Standard ***ISO/IEC 27036-2****:2022, Cybersecurity – Supplier relationships – part 2: Requirements,* which has been prepared by jointly by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC).

Terminology and conventions

Some terminologies and certain conventions are not identical with those used in Tanzania Standards; Attention is drawn especially to the following:

1) The comma has been used as a decimal marker for metric dimensions. In Tanzania Standards, it is current practice to use “full point” on the baseline as the decimal marker.

2) Where the words “International Standard(s)” appear, referring to this standard they should read “Tanzania Standard(s)”.

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see https://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, Information security, cybersecurity and privacy protection.

This second edition cancels and replaces the first edition (ISO/IEC 27036-2:2014), which has been technically revised.

The main changes are as follows:

— the structure and content have been aligned with the most recent version of ISO/IEC 15288.

A list of all parts in the ISO/IEC 27036 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

Organizations throughout the world work with suppliers to acquire products and services. Many organizations establish several supplier relationships to cover a variety of business needs, such as operations or manufacturing. Conversely, suppliers provide products and services to several acquirers.

Relationships between acquirers and suppliers established for the purpose of acquiring a variety of products and services may introduce information security risks to both acquirers and suppliers. These risks are caused by mutual access to the other party's assets, such as information and information systems, as well as by the difference in business objectives and information security approaches. These risks should be managed by both acquirers and suppliers.

This document:

a) specifies fundamental information security requirements for defining, implementing, operating, monitoring, reviewing, maintaining and improving supplier and acquirer relationships;

b) facilitates mutual understanding of the other party's approach to information security and tolerance for information security risks;

c) reflects the complexity of managing risks that can have information security impacts in supplier and acquirer relationships;

d) is intended to be used by any organization willing to evaluate the information security in supplier or acquirer relationships;

e) is not intended for certification purposes;

f) is intended to be used to set a number of defined information security objectives applicable to a supplier and acquirer relationship that is a basis for assurance purposes.

ISO/IEC 27036-1 provides an overview and concepts associated with information security in supplier relationships.

ISO/IEC 27036-3 provides guidelines for the acquirer and the supplier for managing information security risks specific to the ICT products and services supply chain.

ISO/IEC 27036-4 provides guidelines for the acquirer and the supplier for managing information security risks specific to the cloud services.

1 Scope

This document specifies fundamental information security requirements for defining, implementing, operating, monitoring, reviewing, maintaining and improving supplier and acquirer relationships.

These requirements cover any procurement and supply of products and services, such as manufacturing or assembly, business process procurement, software and hardware components, knowledge process procurement, build-operate-transfer and cloud computing services.

This document is applicable to all organizations, regardless of type, size and nature.

To meet the requirements, it is expected that an organization has internally implemented a number of foundational processes or is actively planning to do so. These processes include, but are not limited to: business management, risk management, operational and human resources management, and information security.