DRAFT International Standard

ISO/IEC DIS 27004

Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation

Technologies de l'information — Techniques de sécurité — Management de la sécurité de l'information — Surveillance, mesurage, analyse et évaluation

ICS: 35.030

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2026-06-23

Voting terminates on:
2026-09-15

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 27004:2026(en)

© ISO/IEC 2026

Horizontal document



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**
3.1 Terms and definitions ... 1

4 Structure and overview ... **3**

5 Rationale ... **4**
5.1 The need for measurement ... 4
5.2 Fulfilling the ISO/IEC 27001:2022 requirements ... 4
5.3 Validity of results ... 5
5.4 Benefits ... 5

6 Characteristics ... **6**
6.1 General ... 6
6.2 What to monitor ... 6
6.3 What to measure ... 7
6.4 When to monitor, measure, analyse and evaluate ... 8
6.5 Who will monitor, measure, analyse and evaluate ... 8

7 Types of measures ... **9**
7.1 General ... 9
7.2 Performance measures ... 9
7.3 Effectiveness measures ... 10

8 Processes ... **10**
8.1 General ... 10
8.2 Identify information needs ... 11
8.3 Create and maintain measures ... 12
8.3.1 General ... 12
8.3.2 Identify current security practices that can support information needs ... 12
8.3.3 Develop or update measures ... 13
8.3.4 Document measures and prioritize for implementation ... 14
8.3.5 Keep management informed and engaged ... 14
8.4 Establish procedures ... 15
8.5 Monitor and measure ... 15
8.6 Analyse results ... 16
8.7 Evaluate information security performance and ISMS effectiveness ... 16
8.8 Review and improve monitoring, measurement, analysis and evaluation processes ... 16
8.9 Retain and communicate documented information ... 16

Annex A (informative) **An information security measurement model** ... **18**

Annex B (informative) **Measurement construct examples** ... **20**

Annex C (informative) **An example of free-text form measurement construction** ... **65**

Bibliography ... **66**

© ISO/IEC 2026 – All rights reserved

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

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).

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

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This third edition of ISO/IEC 27004 cancels and replaces the second edition (ISO/IEC 27004:2016), which has been technically revised.

This edition includes the following significant changes with respect to the previous edition:

The text has been modified for alignment with ISO/IEC 27001:2022, specifically:

— the new requirement in ISO/IEC 27001:2022, Clause 6.2 to monitor the information security objectives

— the reordering of the requirements in ISO/IEC 27001:2022, Clause 9.1

— the references to ISO/IEC 27002:2022 in Annex B of this document.

© ISO/IEC 2026 – All rights reserved

Introduction

This document is intended to assist organizations to evaluate the information security performance and the effectiveness of an information security management system. It thereby assists organizations to fulfil the requirements of ISO/IEC 27001:2022, 9.1: monitoring, measurement, analysis and evaluation.

The results of monitoring and measurement of an information security management system (ISMS) can support decisions concerning ISMS governance, management, operational effectiveness and continual improvement.

As with other ISO/IEC 27000 documents, this document should be considered, interpreted and adapted to suit each organization's specific situation. The concepts and approaches are intended to be universally applicable. However, the measures required by an organization depends on factors such as its size, market sector, maturity, information security risks and management style.

This document is recommended for organizations implementing an ISMS that meets the requirements of ISO/IEC 27001:2022. It does not establish any requirements additional to ISO/IEC 27001:2022. Nor does it oblige organizations to apply the guidelines it contains.

© ISO/IEC 2026 – All rights reserved

Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation

1 Scope

This document provides guidelines intended to assist organizations in evaluating the information security performance and the effectiveness of an information security management system (ISMS). It thereby assists organizations to fulfil the requirements of ISO/IEC 27001:2022, Clause 9.1. It establishes:

a) the monitoring and measurement of information security performance;

b) the monitoring and measurement of the effectiveness of an ISMS, including its processes and controls;

c) the analysis and evaluation of the results of monitoring and measurement.

This document excludes any and all aspects of conformity assessment.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at https://www.electropedia.org/

— ISO Online browsing platform: available at https://www.iso.org/obp

3.1.1
base measure
measure (3.1.8) defined in terms of an attribute and the method for quantifying it

Note 1 to entry: A base measure is functionally independent of other *measures*.

[SOURCE: ISO/IEC/IEEE 15939:2017, 3.3, modified — Note 2 to entry has been deleted.]

3.1.2
control
measure that maintains and/or modifies risk

Note 1 to entry: in this standard the notion of “measure” depends on the context where it is being used. Therefore “measure” when referred to a control (see 3.1.2) should not be used as synonym of “measure” (see 3.1.8) which relates to a measurement’ context.”

[SOURCE: ISO/IEC 27002:2022]

© ISO/IEC 2026 – All rights reserved

3.1.3
derived measure
measure (3.1.8) that is defined as a function of two or more values of *base measures* (3.1.1)

[SOURCE: ISO/IEC/IEEE 15939:2017, 3.8, modified — Note 1 to entry has been deleted.]

3.1.4
effectiveness
extent to which planned activities are realized and planned results achieved

3.1.5
effectiveness measure
measure (3.1.8) to express the effect that realization of the planned activities has on the organization's information security objectives

Note 1 to entry: This type of measure is not to be confused with the definition of effectiveness.

[SOURCE: Derived from NIST Special Publication 800-55]

3.1.6
indicator
measure (3.1.8) that provides an estimate or evaluation

3.1.7
information need
insight necessary to manage objectives, goals, risks and problems

[SOURCE: ISO/IEC/IEEE 15939:2017, 3.12]

3.1.8
measure
variable to which a value is assigned as the result of *measurement* (3.1.9)

[SOURCE: ISO/IEC/IEEE 15939:2017, 3.15, modified — Note 2 to entry has been deleted.]

3.1.9
measurement
process to determine a value

3.1.10
measurement function
algorithm or calculation performed to combine two or more *base measures* (3.1.1)

[SOURCE: ISO/IEC/IEEE 15939:2017, 3.13]

3.1.11
measurement method
logical sequence of operations, described generically, used in quantifying an attribute with respect to a specified scale

Note 1 to entry: The type of measurement method depends on the nature of the operations used to quantify an attribute. Two types can be distinguished:

— subjective: quantification involving human judgment; and

— objective: quantification based on numerical rules.

[SOURCE: ISO/IEC/IEEE 15939:2017, 3.21, modified — Note 2 to entry has been deleted.]

3.1.12
monitoring
determining the status of a system, a process or an activity

© ISO/IEC 2026 – All rights reserved

3.1.13
performance
measurable result

3.1.14
performance measure
measure (3.1.8) to express the planned results of some activity in terms of the characteristics of that activity

Note 1 to entry: This type of measure is not to be confused with the definition of performance.

[SOURCE: Derived from NIST Special Publication 800-55]

4 Structure and overview

The structure of this document is:

a) Rationale (Clause 5);

b) Characteristics (Clause 6);

c) Types of measures (Clause 7);

d) Processes (Clause 8).

These clauses map to the ISO/IEC 27001:2022, 9.1 requirements, as illustrated in Figure 1.

To determine what to monitor and measure, organizations should start by determining their information needs. Only then can the organization determine the measures that it requires. The application of these measures produces data which is then analysed. The results of analysis are evaluated in fulfilment of the organization's information needs. An example of an information need is the insight necessary to know whether its information security objectives are being fulfilled (as required by ISO/IEC 27001:2022, 6.2).

In addition, Annex A describes a measurement model for information security. The annex shows the relationship between the measurement model components and the ISO/IEC 27001:2022, 9.1 requirements.

Annex B provides a wide range of examples. These examples are intended to provide practical guidance on how organizations can monitor, measure, analyse and evaluate their chosen ISMS processes and areas of information security performance. These examples use the suggested template given in Table 1. Annex C provides a further example using an alternative free-form text-based format.

© ISO/IEC 2026 – All rights reserved