



# ISO/IEC 27004

Search this site

[Home](#)[ISO27k standards](#)[FREE ISO27k Forum](#)[FREE ISO27k Toolkit](#)[FREE ISO27k FAQ](#)[About us](#)[ISO/IEC 27000](#)[ISO/IEC 27001](#)[ISO/IEC 27002](#)[ISO/IEC 27003](#)[ISO/IEC 27004](#)[ISO/IEC 27005](#)[ISO/IEC 27006](#)[ISO/IEC 27007](#)[ISO/IEC TS 27008](#)[ISO/IEC 27009](#)[ISO/IEC 27010](#)

## [ISO/IEC 27004:2016](#) – Information technology – Security techniques – **Information security management – Monitoring, measurement, analysis and evaluation** (*second edition*)

### Introduction

ISO/IEC 27004 concerns measurements or measures needed for information security management: these are commonly known as 'security metrics' in the profession (if not within ISO/IEC JTC 1/SC 27!).

### Scope and purpose

The standard is intended to help organizations evaluate the effectiveness and efficiency of their ISO27k Information Security Management Systems, providing information necessary to manage and (where necessary) improve the ISMS systematically. It expands substantially on clause 9.1 of [ISO/IEC 27001](#) concerning 'monitoring, measurement, analysis and evaluation'.

ISO/IEC 27011

ISO/IEC 27013

ISO/IEC 27014

ISO/IEC TR 27016

ISO/IEC 27017

ISO/IEC 27018

ISO/IEC TR 27019

ISO/IEC 27021

ISO/IEC 27022

ISO/IEC TR 27023

ISO/IEC 27030

ISO/IEC 27031

ISO/IEC 27032

ISO/IEC 27033

ISO/IEC 27034

ISO/IEC 27035

ISO/IEC 27036

ISO/IEC 27037

ISO/IEC 27038

ISO/IEC 27039

## Content

These are the main sections:

5. Rationale - explains the value of measuring stuff e.g. to increase accountability and performance;
6. Characteristics - what to measure, monitor, analyze and evaluate, when to do it, and who to do it;
7. Types of measures - performance (efficiency) and effectiveness measures;
8. Processes - how to develop, implement and use metrics.

Annex A is where most of the theoretical measurement model from the 2009 version of the standard now languishes.

Annex B catalogs 35 metrics examples of varying utility and quality, using a typical metrics definition form.

Annex C demonstrates a pseudo-mathematical way to describe a metric, or rather an 'effectiveness measurement construct' (!).

## Status of the standard

The standard was first published in **2009**.

A substantially revised (rewritten) second edition was **published in 2016**.

A handful of minor typographical issues will soon be addressed through a corrigendum.

## Personal comments

In contrast to the rather academic/theoretical 2009 release, the 2016 second edition of this standard is *much* more pragmatic and hence useful for infosec practitioners.

An ISMS is literally worse than useless without suitable metrics (thus it is appropriate for [ISO/IEC 27001](#) to list this standard as a normative or essential standard) but information security metrics are of value in *all* organizations regardless of whether or not they have an ISO27k ISMS in place. I understand why the revised 27004 standard (along with several [other ISO27k standards](#)) are aligned specifically to [27001](#): the narrow scope and tight focus increases the chances of the standards being completed and published in a reasonable timeframe (a problem that plagued the original version of 27004, and derailed the [27005](#) revision). However, I believe that leaves a gap

[ISO/IEC 27040](#)[ISO/IEC 27041](#)[ISO/IEC 27042](#)[ISO/IEC 27043](#)[ISO/IEC 27045](#)[ISO/IEC 27050](#)[ISO/IEC 27070](#)[ISO/IEC 27071](#)[ISO/IEC 27099](#)[ISO/IEC TS 27100](#)[ISO/IEC 27101](#)[ISO/IEC 27102](#)[ISO/IEC TR 27103](#)[ISO/IEC TR 27550](#)[ISO/IEC 27551](#)[ISO/IEC 27553](#)[ISO/IEC 27554](#)[ISO/IEC 27555](#)[ISO/IEC 27556](#)[ISO/IEC TS 27570](#)

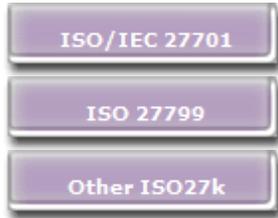
for broader-scope standards, including a general purpose information risk and security metrics standard ... or indeed [an entire book](#).

The example metrics in Annex B are a mixed bunch, and are not very well described. Please don't think that you ought to be using them, unless they happen to suit your specific information needs. In most cases, there are better ways to measure - better security metrics.

Various metrics-related terms from the 2009 version of the standard are defined in [ISO/IEC 27000](#) but are mostly irrelevant now. They may be dropped when 27000 is next updated.

The German standards body, DIN, suggested introducing the [GQM \(Goal-Question-Metric\) approach](#) into the standard - an excellent idea but raised far too late in the revision project to make it into the 2016 release. I hope it will resurface in the *next* round of revision.

< [Previous standard](#)    ^ [Up a level](#) ^    [Next standard](#) >



Copyright © 2019 IsecT Ltd.