ISO/IEC 27004

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

Abstract

Summary podcast

"ISO/IEC 27004:2016 provides guidelines intended to assist organisations in evaluating the information security performance and the effectiveness of an information security management system in order to fulfil the requirements of ISO/IEC 27001:2013, 9.1. It establishes: (a) the monitoring and measurement of information security performance; (b) the monitoring and measurement of the effectiveness of an information security management system (ISMS) including its processes and controls; [and] (c) the analysis and evaluation of the results of monitoring and measurement."

[Source: ISO/IEC 27004:2016]

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 an organisation evaluate the effectiveness and efficiency of its **I**nformation **S**ecurity **M**anagement **S**ystem, 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'.

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, analyse 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.

ISO/IEC 27036
ISO/IEC 27037
ISO/IEC 27038
ISO/IEC 27039
ISO/IEC 27040
ISO/IEC 27041
ISO/IEC 27042
ISO/IEC 27043
ISO/IEC 27045
ISO/IEC 27046
ISO/IEC 27050
ISO/IEC 27070
ISO/IEC 27071
ISO/IEC 27090
ISO/IEC 27091
ISO/IEC 27099
ISO/IEC TS 27100
ISO/IEC 27102
ISO/IEC TR 27103
ISO/IEC TR 27109
ISO/IEC TS 27110
ISO/IEC TS 27115
ISO/IEC 27116
ISO/IEC 27400
ISO/IEC 27402
ISO/IEC 27403
ISO/IEC 27404
ISO/IEC TR 27550
ISO/IEC 27551
ISO/IEC 27553
ISO/IEC 27554
ISO/IEC 27555
ISO/IEC 27556
ISO/IEC 27557
ISO/IEC 27559
ISO/IEC TS 27560

Annex A is where most of the theoretical measurement model from the *first* edition 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 *first* edition was published in **2009**.

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

Work is under way on a *third* edition. The committee SC 27 plans to:

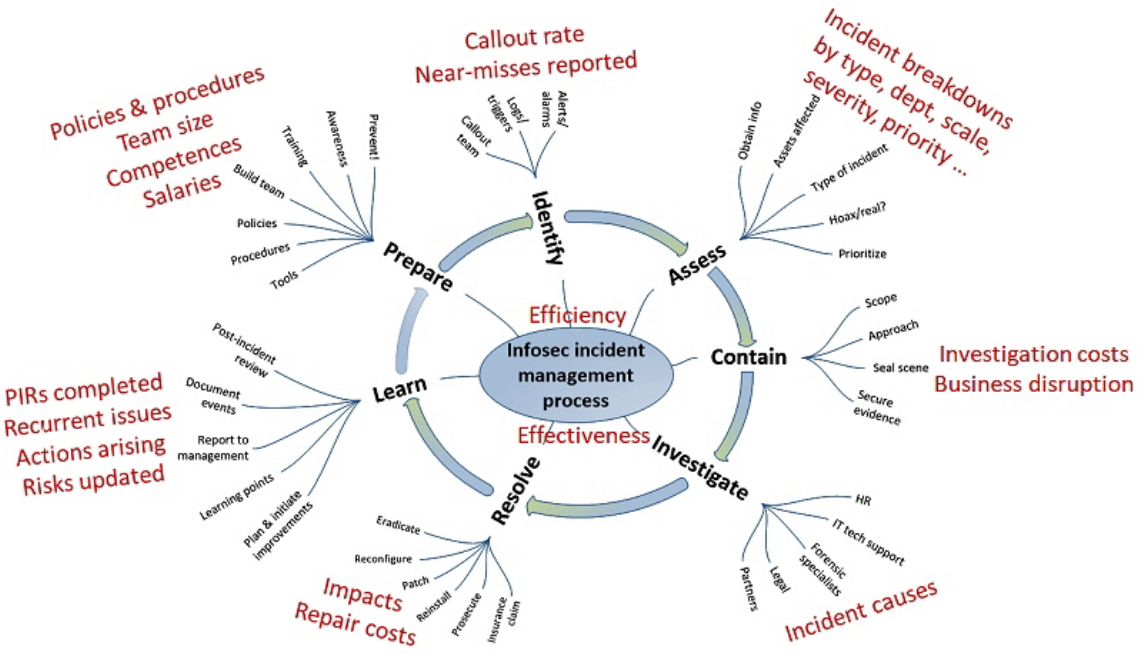
1. Update the main body and appendix references to reflect the 2022 editions of ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27005.
2. Adopt ISO's version of plain English. This *may* involve *extensive* wording changes to make the standard easier to understand and apply.
3. Provide additional metrics examples to suit organisations of all sizes.

If all goes to plan, the third edition will be published before 2028.

Personal comments

Since a management system is literally worse than useless without suitable metrics, it is appropriate for ISO/IEC 27001 to list this standard as a normative or essential standard. More than that, information security metrics are of value in *all* organisations regardless of whether or not they have an ISO27k ISMS in place. I understand why ISO/IEC 27004 and several other ISO27k standards are aligned specifically to ISO/IEC 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 first edition of ISO/IEC 27004). That leaves a gap 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 of the current second edition are a mixed bunch, and are not very well described. Please don't think that you ought to be using them in your ISMS, unless they happen to address your specific management information needs. There are *lots* of moving parts to an ISMS, numerous objectives and hence plenty of measurable aspects. For example, here are some possible metrics relating solely to the incident management process*:*



The German standards body, DIN, suggested introducing the GQM (**G**oal-**Q**uestion-**M**etric) approach into the standard - an excellent idea raised too late for the *second* edition. Unfortunately, it seems the current revision is once again missing the opportunity for this worthwhile improvement. Meanwhile, Lance Hayden's book "IT Security Metrics" ably explains using GQM to identify possible metrics, while "PRAGMATIC Security Metrics" by

ISO/IEC 27561
ISO/IEC 27562
ISO/IEC TR 27563
ISO/IEC 27564
ISO/IEC 27565
ISO/IEC 27566
ISO/IEC 27568
ISO/IEC 27569
ISO/IEC TS 27570
ISO/IEC 27573
ISO/IEC 27701
ISO/IEC 27706
ISO 27799

Brotby and Hinson describes a systematic method to evaluate and improve their quality.

Various obscure metrics-related terms from the first edition of the standard are defined in ISO/IEC 27000 but are mostly irrelevant now. Hopefully they will be dropped when ISO/IEC 27000 is updated.

< Previous standard ^ Up a level ^ Next standard >