SVENSK STANDARD
SS-ISO/IEC 27004:2010

Fastställd/Approved: 2010-01-25
Publicerad/Published: 2010-02-23
Utgåva/Edition: 1
Språk/Language: engelska/English
ICS: 01.140.30; 04.050; 35.020; 35.040; 35.240.01

Informationsteknik – Säkerhetstekniker – Styrning av informationssäkerhet – Mätning (ISO/IEC 27004:2009, IDT)

Information technology – Security techniques – Information security management – Measurement (ISO/IEC 27004:2009, IDT)

SWEDISH STANDARDS INSTITUTE

Hitta rätt produkt och ett leveranssätt som passar dig

Standarder
Genom att följa gällande standard både effektiviserar och säkrar du ditt arbete. Många standarder ingår dessutom ofta i paket.

Tjänster
Abonnemang är tjänsten där vi uppdaterar dig med aktuella standarder när förändringar sker på dem du valt att abonnera på. På så sätt är du säker på att du alltid arbetar efter rätt utgåva.
e-nav är vår online-tjänst som ger dig och dina kollegor tillgång till standarder ni valt att abonnera på dygnet runt. Med e-nav kan samma standard användas av flera personer samtidigt.

Leveranssätt
Du väljer hur du vill ha dina standarder levererade. Vi kan erbjuda dig dem på papper och som pdf.

Andra produkter
Vi har böcker som underlättar arbetet att följa en standard. Med våra böcker får du ökad förståelse för hur standarder ska följas och vilka fördelar den ger dig i ditt arbete. Vi tar fram många egna publikationer och fungerar även som återförsäljare. Det gör att du hos oss kan hitta över 500 unika titlar. Vi har även tekniska rapporter, specifikationer och "workshop agreement". Matriser är en översikt på standarder och handböcker som bör läsas tillsammans. De finns på sis.se och ger dig en bra bild över hur olika produkter hör ihop.

Standardiseringsprojekt
Du kan påverka innehållet i framtida standarder genom att delta i någon av SIS ca 400 Tekniska Kommittéer.

Find the right product and the type of delivery that suits you

Standards
By complying with current standards, you can make your work more efficient and ensure reliability. Also, several of the standards are often supplied in packages.

Services
Subscription is the service that keeps you up to date with current standards when changes occur in the ones you have chosen to subscribe to. This ensures that you are always working with the right edition.
e-nav is our online service that gives you and your colleagues access to the standards you subscribe to 24 hours a day. With e-nav, the same standards can be used by several people at once.

Type of delivery
You choose how you want your standards delivered. We can supply them both on paper and as PDF files.

Other products
We have books that facilitate standards compliance. They make it easier to understand how compliance works and how this benefits you in your operation. We produce many publications of our own, and also act as retailers. This means that we have more than 500 unique titles for you to choose from. We also have technical reports, specifications and workshop agreements. Matrices, listed at sis.se, provide an overview of which publications belong together.

Standardisation project
You can influence the content of future standards by taking part in one or other of SIS's 400 or so Technical Committees.

Den internationella standarden ISO/IEC 27004:2009 gäller som svensk standard. Detta dokument innehåller den officiella engelska versionen av ISO/IEC 27004:2009.

The International Standard ISO/IEC 27004:2009 has the status of a Swedish Standard. This document contains the official English version of ISO/IEC 27004:2009.

Upplysningar om sakinnehållet i standarden lämnas av SIS, Swedish Standards Institute, telefon 08-555 520 00.
Standarder kan beställas hos SIS Förlag AB som även lämnar allmänna upplysningar om svensk och utländsk standard.

Information about the content of the standard is available from the Swedish Standards Institute (SIS), tel +46 8 555 520 00.
Standards may be ordered from SIS Förlag AB, who can also provide general information about Swedish and foreign standards.

SIS Förlag AB, SE 118 80 Stockholm, Sweden. Tel: +46 8 555 523 10. Fax: +46 8 555 523 11.
E-mail: sis.sales@sis.se Internet: www.sis.se

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

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 27004 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

0 Introduction

0.1 General

This International Standard provides guidance on the development and use of measures and measurement in order to assess the effectiveness of an implemented information security management system (ISMS) and controls or groups of controls, as specified in ISO/IEC 27001.

This would include policy, information security risk management, control objectives, controls, processes and procedures, and support the process of its revision, helping to determine whether any of the ISMS processes or controls need to be changed or improved. It needs to be kept in mind that no measurement of controls can guarantee complete security.

The implementation of this approach constitutes an Information Security Measurement Programme. The Information Security Measurement Programme will assist management in identifying and evaluating non-compliant and ineffective ISMS processes and controls and prioritizing actions associated with improvement or changing these processes and/or controls. It may also assist the organization in demonstrating ISO/IEC 27001 compliance and provide additional evidence for management review and information security risk management processes.

This International Standard assumes that the starting point for the development of measures and measurement is a sound understanding of the information security risks that an organization faces, and that an organization's risk assessment activities have been performed correctly (i.e. based on ISO/IEC 27005), as required by ISO/IEC 27001. The Information Security Measurement Programme will encourage an organization to provide reliable information to relevant stakeholders concerning its information security risks and the status of the implemented ISMS to manage these risks.

Effectively implemented, the Information Security Measurement Programme would improve stakeholder confidence in measurement results, and enable the stakeholders to use these measures to effect continual improvement of information security and the ISMS.

The accumulated measurement results will allow comparison of progress in achieving information security objectives over a period of time as part of an organization's ISMS continual improvement process.

0.2 Management overview

ISO/IEC 27001 requires the organization to "undertake regular reviews of the effectiveness of the ISMS taking into account results from effectiveness measurement" and to "measure the effectiveness of controls to verify that security requirements have been met". ISO/IEC 27001 also requires the organization to "define how to measure the effectiveness of the selected controls or groups of controls and specify how these measures are to be used to assess control effectiveness to produce comparable and reproducible results".

The approach adopted by an organization to fulfil the measurement requirements specified in ISO/IEC 27001 will vary based on a number of significant factors, including the information security risks that the organization faces, its organizational size, resources available, and applicable legal, regulatory and contractual requirements. Careful selection and justification of the method used to fulfil the measurement requirements are important to ensure that excessive resources are not devoted to these activities of the ISMS to the detriment of others. Ideally, ongoing measurement activities are to be integrated into the regular operations of the organization with minimal additional resource requirements.

This International Standard gives recommendations concerning the following activities as a basis for an organization to fulfil measurement requirements specified in ISO/IEC 27001:

a) developing measures (i.e. base measures, derived measures and indicators);

b) implementing and operating an Information Security Measurement Programme;
c) collecting and analysing data;
d) developing measurement results;
e) communicating developed measurement results to the relevant stakeholders;
f) using measurement results as contributing factors to ISMS-related decisions;
g) using measurement results to identify needs for improving the implemented ISMS, including its scope, policies, objectives, controls, processes and procedures; and
h) facilitating continual improvement of the Information Security Measurement Programme.

One of the factors that will impact the organization's ability to achieve measurement is its size. Generally the size and complexity of the business in combination with the importance of information security affect the extent of measurement needed, both in terms of the numbers of measures to be selected and the frequency of collecting and analysing data. For SMEs (Small and Medium Enterprises) a less comprehensive information security measurement program will be sufficient, whereas large enterprises will implement and operate multiple Information Security Measurement Programmes.

A single Information Security Measurement Programme may be sufficient for small organizations, whereas for large enterprises the need may exist for multiple Information Security Measurement Programmes.

The guidance provided by this International Standard will result in the production of documentation that will contribute to demonstrating that control effectiveness is being measured and assessed.

Information technology — Security techniques — Information security management — Measurement

1 Scope

This International Standard provides guidance on the development and use of measures and measurement in order to assess the effectiveness of an implemented information security management system (ISMS) and controls or groups of controls, as specified in ISO/IEC 27001.

This International Standard is applicable to all types and sizes of organization.

NOTE This document uses the verbal forms for the expression of provisions (e.g. “shall”, “shall not”, “should”, “should not”, “may”, “need not”, “can” and “cannot”) that are specified in the ISO/IEC Directives, Part 2, 2004, Annex H. See also ISO/IEC 27000:2009, Annex A.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000:2009, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

3.1
analytical model
algorithm or calculation combining one or more base and/or derived measures with associated decision criteria

[ISO/IEC 15939:2007]

3.2
attribute
property or characteristic of an object that can be distinguished quantitatively or qualitatively by human or automated means

[ISO/IEC 15939:2007]

3.3
base measure
measure defined in terms of an attribute and the method for quantifying it

[ISO/IEC 15939:2007]

NOTE A base measure is functionally independent of other measures.