Teknisk rapport
SIS-ISO/IEC TR 27016:2018

Publicerad/Published: 2018-03-15
Utgåva/Edition: 1
Språk/Language: engelska/English
ICS: 35.040

IInformationsteknik - Säkerhetstekniker - Hantering av informationssäkerhet - Ekonomiska aspekter (ISO/IEC TR 27016:2014, IDT)

Information technology - Security techniques - Information security management - Organizational economics (ISO/IEC TR 27016:2014, IDT)

Standarder får världen att fungera

SIS (Swedish Standards Institute) är en fristående ideell förening med medlemmar från både privat och offentlig sektor. Vi är en del av det europeiska och globala nätverk som utarbetar internationella standarder. Standarder är dokumenterad kunskap utvecklad av framstående aktörer inom industri, näringsliv och samhälle och befrämjar handel över gränser, bidrar till att processer och produkter blir säkrare samt effektiviserar din verksamhet.

Delta och påverka
Som medlem i SIS har du möjlighet att påverka framtida standarder inom ditt område på nationell, europeisk och global nivå. Du får samtidigt tillgång till tidig information om utvecklingen inom din bransch.

Ta del av det färdiga arbetet
Vi erbjuder våra kunder allt som rör standarder och deras tillämpning. Hos oss kan du köpa alla publikationer du behöver – allt från enskilda standarder, tekniska rapporter och standard-paket till handböcker och onlinetjänster. Genom vår webbtjänst e-nav får du tillgång till ett lättnavigerat bibliotek där alla standarder som är aktuella för ditt företag finns tillgängliga. Standarder och handböcker är källor till kunskap. Vi säljer dem.

Utveckla din kompetens och lyckas bättre i ditt arbete
Hos SIS kan du gå öppna eller företagsinterna utbildningar kring innehåll och tillämpning av standarder. Genom vår närhet till den internationella utvecklingen och ISO får du rätt kunskap i rätt tid, direkt från källan. Med vår kunskap om standarders möjligheter hjälper vi våra kunder att skapa verklig nytta och lönsamhet i sina verksamheter.

Vill du veta mer om SIS eller hur standarder kan effektivisera din verksamhet är du välkommen in på www.sis.se eller ta kontakt med oss på tel 08-555 523 00.

Standards make the world go round

SIS (Swedish Standards Institute) is an independent non-profit organisation with members from both the private and public sectors. We are part of the European and global network that draws up international standards. Standards consist of documented knowledge developed by prominent actors within the industry, business world and society. They promote cross-border trade, they help to make processes and products safer and they streamline your organisation.

Take part and have influence
As a member of SIS you will have the possibility to participate in standardization activities on national, European and global level. The membership in SIS will give you the opportunity to influence future standards and gain access to early stage information about developments within your field.

Get to know the finished work
We offer our customers everything in connection with standards and their application. You can purchase all the publications you need from us - everything from individual standards, technical reports and standard packages through to manuals and online services. Our web service e-nav gives you access to an easy-to-navigate library where all standards that are relevant to your company are available. Standards and manuals are sources of knowledge. We sell them.

Increase understanding and improve perception
With SIS you can undergo either shared or in-house training in the content and application of standards. Thanks to our proximity to international development and ISO you receive the right knowledge at the right time, direct from the source. With our knowledge about the potential of standards, we assist our customers in creating tangible benefit and profitability in their organisations.

If you want to know more about SIS, or how standards can streamline your organisation, please visit www.sis.se or contact us on phone +46 (0)8-555 523 00

Denna tekniska rapport är inte en svensk standard. Detta dokument innehåller den engelska språkversionen ISO/IEC TR 27016:2014.

This Technical Report is not a Swedish Standard. This document contains the English version of ISO/IEC TR 27016:2014.

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

Information about the content of this document is available from the SIS, Swedish Standards Institute, telephone +46 8 555 520 00. Standards may be ordered from SIS, who can also provide general information about national and international standards.

Detta dokument är framtaget av kommittén för LIS, SIS/TK 318/AG 11.

Har du synpunkter på innehållet i det här dokumentet, vill du delta i ett kommande revideringsarbete eller vara med och ta fram standarder inom området? Gå in på www.sis.se - där hittar du mer information.

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.

In exceptional circumstances, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide to publish a Technical Report. A Technical Report is entirely informative in nature and shall be subject to review every five years in the same manner as an International Standard.

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 TR 27016 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

This Technical Report provides guidelines on information security economics as a decision making process concerning the production, distribution, and consumption of limited goods and services. Actions for the protection of an organization's information assets require resources, which otherwise could be allocated to alternative non-information security related uses. The reader of this Technical Report is primarily intended to be executive management who have delegated responsibility from the governing body for strategy and policy, e.g. Chief Executive Officers (CEOs), Heads of Government Organizations, Chief Financial Officers (CFOs), Chief Operating Officers (COOs), Chief Information Officers (CIOs), Chief Information Security Officers (CISOs) and similar roles.

Information security management is often seen as an information technology only approach using technical controls (e.g. encryption, access and privilege management, firewalls, and intrusion and malicious code eradication). However, any application of information security is not effective without considering a broad range of other controls (e.g. physical controls, human resource controls, policies and rules, etc.). A decision has to be made to allocate sufficient resources to support a broad range of controls as part of information security management. This Technical Report supports the broad objectives of information security as provided in the ISO/IEC 27000 family of standards by introducing economics as a key component of the decision making process.

Coupled with a risk management approach (ISO/IEC 27005[5]) and the ability to perform information security measurements (ISO/IEC 27004[4]), economic factors need to be considered as part of information security management when planning, implementing, maintaining and improving the security of the organization's information assets. In particular, economic justifications are required to ensure spending on information security is effective as opposed to using the resources in a less efficient way.

Typically, economic benefits of information security management concern one or more of the following:

a) minimizing any negative impact to the organization's business objectives;

b) ensuring any financial loss is acceptable;

c) avoiding requirements for additional risk capital and contingency provisioning.

Information security management may also produce benefits that are not driven by financial concerns alone. While these non-financial benefits are important, they are usually excluded from financial based economic analysis. Such benefits need to be quantified and included as part of the economic analysis. Examples include:

a) enabling the business to participate in high-risk endeavours;

b) enabling the business to satisfy legal and regulatory obligations;

c) managing customer expectations of the organization;

d) managing community expectations of the organization;

e) maintaining a trusted organizational reputation;

f) providing assurance of completeness and accuracy of financial reporting.

Negative financial and non-financial economic impacts as a result of a failure by the organization to provide adequate protection of its information assets are increasingly becoming a business issue. The value of information security management includes identifying a direct relationship between the cost of controls to prevent loss, and the cost benefit of avoiding a loss.

Increasing levels of competition are resulting in the need for organizations to focus on the economics of risk.

This Technical Report supplements the ISO/IEC 27000 family of standards by overlaying an economic perspective on protecting an organization's information assets in the context of the wider societal environment in which an organization operates.

Information technology — Security techniques — Information security management — Organizational economics

1 Scope

This Technical Report provides guidelines on how an organization can make decisions to protect information and understand the economic consequences of these decisions in the context of competing requirements for resources.

This Technical Report is applicable to all types and sizes of organizations and provides information to enable economic decisions in information security management by top management who have responsibility for information security decisions.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

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
annualized loss expectancy
ALE
monetary *loss* (3.13) that can be expected for an asset due to a risk over a one year period

Note 1 to entry: ALE is defined as: ALE = SLE × ARO, where SLE is the Single Loss Expectancy and ARO is the Annualized Rate of Occurrence.

3.2
direct value
value that can be determined by a value of an identical replacement or substitute in the event of an information asset or assets being harmed or lost

Note 1 to entry: This value is positive as long as the information asset is not harmed but seen as loss if the event occurs.

3.3
economic factor
item or information that affects an asset's *value* (3.22)

3.4
economic comparison
consideration of competing or alternative cases for the allocation of resource

3.5
economic justification
element of business case desiged to enable the allocation of resource

3.6
economic value added
measure that compares net operating profit to total cost of capital

3.7
economics
efficient use of limited resources

3.8
expected value
value estimated as an impact to the business by an information asset being harmed or lost

Note 1 to entry: This value is positive as long as the information asset is not harmed but seen as loss if the event occurs.

3.9
extended value
expected value times the number of times that value might occur

3.10
indirect value
value that is estimated for the replacement or restoring in the event of an information asset or assets being harmed or lost

Note 1 to entry: This value is positive as long as the information asset is not harmed but seen as negative if the event occurs.

3.11
information security economics
efficient use of limited resources for information security management

3.12
information security management
ISM
managing the preservation of confidentiality, integrity and availability of information

3.13
loss
reduction in the *value* (3.22) of an asset

Note 1 to entry: In terms of *information security economics* (3.11), a loss may also be used in the context as a positive value. In this document a cost is always negative unless otherwise stated.

3.14
market value
highest price that a ready, willing and able buyer will pay and the lowest price a seller will accept

3.15
net present value
sum of the *present values* (3.16) of the individual cash flows of the same entity

3.16
present value
current worth of a future sum of money or stream of cash flows given a specified rate of return

3.17
non economic benefit
benefit for which no payment has been made

3.18
opportunity cost
future estimated cost for a certain information security activity or activities

3.19
opportunity value
future estimated positive value gained from a certain information security activity or activities

3.20
regulatory requirements
mandatory resource demands associated with a specific market

3.21
return on investment
measurement per period rates of return on value invested in an economic entity

3.22
societal value
public distinction between right and wrong

3.23
value
relative worth of an asset to other objects or a defined absolute value

Note 1 to entry: In terms of *information security economics* (3.11) a value may be positive or negative. In this document a value is always positive unless otherwise stated.

3.24
value-at-risk
VAR
summarizes the worst *loss* (3.13) over a target time that will not be exceeded with a given probability

Note 1 to entry: Target time for example could be 1 year and the given probability could also be referred to as confidence level.

4 Abbreviated terms

BVM	Basic Value Model
CIA	Confidentiality–Integrity–Availability
ICT	Information and Communications Technology
IRP	Interest Rate Parity
ISMS	Information Security Management System
ROI	Return On Investment

5 Structure of this Document

Fundamental to the organizational economics of information security management is the ability to enable economic values to be presented to management thereby enabling better factual based decisions regarding the resources to be applied to the protection of the organization's information assets.

In this Technical Report Clause 6 descibes information security economic factors and their relevance in management decision making. Clause 7 describes the economic objectives in terms of asset evaluations. Clause 8 describes how to apply an economic balance using information security benefits and costs in an organizational context in general and using examples depending on the category of a business case.