PD ISO/IEC TR 27016:2014

BSI Standards Publication

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

bsi.

...making excellence a habit.™

Document Sharing Hub

National foreword

This Published Document is the UK implementation of ISO/IEC TR 27016:2014.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2014. Published by BSI Standards Limited 2014

ISBN 978 0 580 74023 7

ICS 35.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 28 February 2014.

Amendments issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 27016:2014

TECHNICAL REPORT

ISO/IEC TR 27016

First edition
2014-03-01

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

Technologies de l'information — Techniques de sécurité — Management de la sécurité de l'information — Économie organisationnelle

Reference number
ISO/IEC TR 27016:2014(E)

Documents
Document Sharing Hub
© ISO/IEC 2014

Full document details: PD ISO/IEC TR 27016:2014

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2014

All rights reserved. Unless otherwise specified, 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
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 27016:2014

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviated terms **3**
5 Structure of this Document **3**
6 Information Security Economic Factors **4**
6.1 Management Decisions 4
6.2 Business Cases 4
6.3 Stakeholder Interests 7
6.4 Economic Decision Review 8
7 Economic Objectives **8**
7.1 Introduction 8
7.2 Information Asset Valuations 8
8 Balancing Information Security Economics for ISM **10**
8.1 Introduction 10
8.2 Economic Benefits 11
8.3 Economic Costs 11
8.4 Applying Economic Calculations to ISM 12
Annex A (informative) **Identification of Stakeholders and Objectives for Setting Values** **17**
Annex B (informative) **Economic Decisions and Key Cost Decision Factors** **19**
Annex C (informative) **Economic Models Appropriate for Information Security** **22**
Annex D (informative) **Business Cases Calculation Examples** **26**
Bibliography **31**

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 27016:2014

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*.

© ISO/IEC 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 27016:2014

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.

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 27016:2014

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.

© ISO/IEC 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 27016:2014

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

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 27016:2014

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

© ISO/IEC 2014 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 27016:2014

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.

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 27016:2014

These clauses are supported by a number of annexes:

— Annex A describes wide context objectives of stakeholders regarding the values of information security.

— Annex B describes business objectives and related information security organizational cost issues.

— Annex C describes a set of models that can be used for information security organizational economics.

— Annex D describes examples of using models with example figures.

6 Information Security Economic Factors

6.1 Management Decisions

The ISO/IEC 27000 family of standards provides a number of business related objectives guiding management decisions by which organizations formally and informally assess their need to invest in information security. These management decisions will be made more effective if a relevant process is devised to compare the net benefit of an information security investment with competing demands for resource in other areas of the organization.

The information security decision process needs to include a clear basis in support of management decision-making, taking into account appropriate factors with respect to the organization's information security economics. The economic value of an information security investment should take account of the organization's business objectives. With the business objectives directly linked, other factors such as risks, costs and benefits can now be applied allowing their more effective measurement.

Determining a suitable economic justification for the allocation of resources to preserve the security of information assets, in a way that allows economic comparison with other ways of using the resources, needs to be considered by management. One principle is to apply an approach of resource allocation (e.g. Net Present Value, Return On Investment, Economic Value Added) to an information security management programme in order to produce results that can be compared for decision-making purposes.

a) Some benefits of an information security management programme may not be economic in nature because it is difficult to objectively and consistently measure the benefits in economic terms. For example, if there are regulatory requirements to protect or provide certain information, it may not be possible to determine the economic value of this benefit. This is also referred to as value of compliance.

b) Similarly, the societal value of an information security management programme cannot be objectively determined in economic terms without an effective feedback mechanism from the community. Non-economic benefits are an important part of the justification of an information security management programme, however, they cannot be included in any form of financial economic analysis as it is difficult to apply consistent measurement.

c) Information security can be applied to protect intangible assets such as brand, reputation, etc. The extent of this protection needs to be calculated and presented in such a way that it relates to the organization's evaluation of such intangible assets. The economics applied of the evaluation should be related to the effect of applying information security to the intangible asset. Economic values should be sourced from business functions such as financial, risk management, sales and marketing, etc. Costs for protection should be calculated based on information security.

6.2 Business Cases

An information security investment business case allows an organization to consider whether the economic benefits outweigh the costs and if so by how much. When information security objectives are presented to an organization's management, usually in the form of a business case, economic aspects should be considered. This should include the consequences resulting from considering the information security aspects of a business proposition. For example, what will be the economic impact on the

© ISO/IEC 2014 – All rights reserved
AVA Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 27016:2014

organization's ability to meet its objectives if an activity is (not) done? A business case should aim to provide a clear answer to this question.

The business case should present a balanced cost–benefit-risk view so that the organization is aware of the options and implications of any decision, thus enabling a basis upon which the desirability of a given security investment can be considered to achieve the best outcomes. These implications and options could be positive in terms of correct information security investments or negative if inadequate investments are made.

The business case should be considered in terms of the information security investment costs against any costs associated with risks. The key fundamental elements of the business case should provide decision makers with sufficient information to understand:

a) The value of the information asset.

b) The potential risks to the information asset.

c) The known cost of protecting the information asset.

d) The reduction of risk in relation to applying protection.

At some point the protection costs applied to the value of the information asset will reach an optimum balance point. This optimum point between the protection costs is when the reduction of risk that will affect the value will be less than the cost of protection (see also model C.4).

Figure 1 symbolizes the need for the business case to include economic factors as part of the business process.

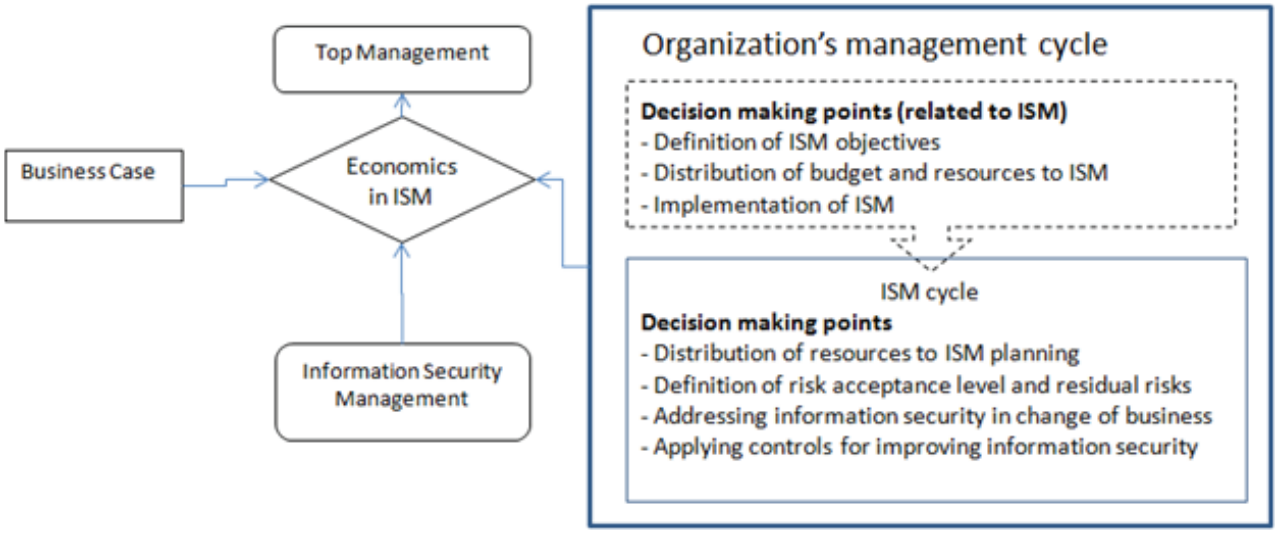

Figure 1 — Information security organizational economics decision process using 27016

When preparing the business case the organization needs to be mindful that resources are always finite and that areas of concern need to be considered and prioritised dependent on the organization's needs. In this context, information security aspects should be founded on facts and hard data where available and calculations should be made based on best knowledge and experience, which may include:

e) Calculation with a time-span (maximum, minimum time period, etc.).

f) Cost estimates.

g) Quotations.

h) Predictions of market values.

© ISO/IEC 2014 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 27016:2014