PD ISO/IEC TR 27016:2014



BSI Standards Publication

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

bsi.

...making excellence a habit.™

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

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)

© ISO/IEC 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

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

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

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

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

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