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 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

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.

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

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.

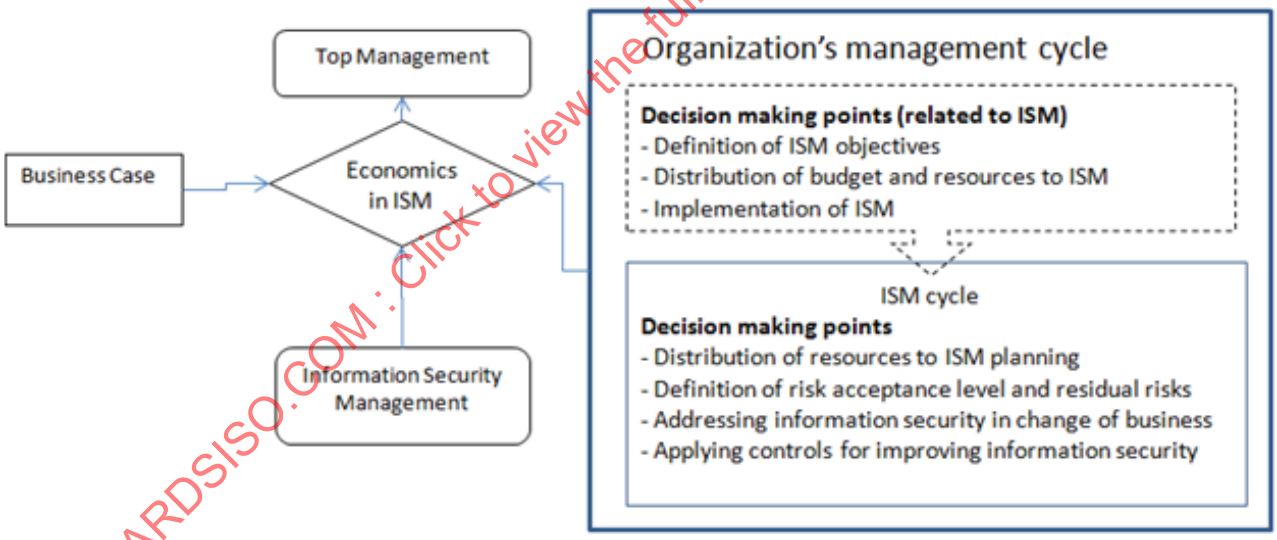

Figure 1 — Information security organizational economics decision process using 27016

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.

i) Known or estimated noncompliance fees and penalties.

j) Legal consequences in direct or indirect economic terms.

k) Risk estimates that provide predictions of losses occurring.

l) Opportunity Value.

m) Opportunity Cost.

When making estimates based on a time-span, these could be gathered from statistics, risk assesments, etc. When defining a time-span it is useful to consult experts from all relevant functions and areas.

Economics related to information security management should cover:

n) Activities and decisions during the whole information security management process.

o) Economic aspects supporting the decision on annual investments for the information security management process.

p) Ensuring that information security management is undertaken in conformity with ISO/IEC 27001[1] (information security management system).

The complexity of a business case for information security management is dependent on scope which in turn, is based on the context in which information security needs to be applied. In order to be able to include information security organizational economics as part of a business case, a business rationale based on a business description needs to be considered in combination with the actual information security solution. Different economic models can be applied to business cases at different levels of the organization. These levels could be as simple as using two categories: Category A - Organizational and Category B - Part of the organization consisting of a process, function, etc. The organizational part can contain a number of assets. From an information security management perspective, Category B could also be an application business case for a control or controls.

Table 1 — Categorization of business cases

Business case category	Type/Scope	Description of type of business case	ISM example	Calculation characteristics
A	Organization wide	High level and more conceptual. This means that the case describes information security applied to the whole or a major part of the organization.	A typical case is an ISMS implementation or merger or acqusition of another organization. It assumed that ISMS 'organization wide' applies to the agreed scope boundaries	High level calculation of opportunity values for the organization and costs for implementing and running the business case. A range is recommended for both values and costs.
B	Part of the organization such as process/department/ function and/or asset/assets and/ or control/controls	A case based on a business activity or an information security activity. The case concerns a change to part of the business and describes information security applied to the change and investment for the organization with multiple effects on information security. The case describes information security applied to a specific asset or set of assetswhere one or a number of controls should be applied.	A typical case is an ICT outsourcing, computer centre and/or such items as secure web, enhanced perimeter protection, computer centre fire protection, IDS deployment, etc.	There could be several calculations and results may need to be aggregated. A calculation of values and costs is generally easy to define but may need to be estimated for complex business cases. A range is recommended for estimates of values but not costs.

Further information about economic decisions and key decision factors are described in Annex B.

6.3 Stakeholder Interests

ISO/IEC 27001[1] stipulates that the ISMS should be used to further stakeholders' interests. Furthering these interests should include consideration of information security economics. Economic factors should be considered where information security could have a negative impact on stakeholders. As an example the following values may be used:

a) Societal value, for example, should the total economic value of the defined society be included or should there be any limitations?

b) Brand value, key business value, etc.

c) Reputation.

d) Customer value.

e) IPR (Intellectual Property Rights).

f) Depending on the business, particular economic values may be needed such as within the health care sector, transport sector, etc.

Other functions within an organization may have already considered these values for their own economic calculations and should be encouraged to provide valuable input when information security is being considered.

Further information on stakeholders and their objectives are found in Annex A.

6.4 Economic Decision Review

The implementation and ongoing management of information security controls to protect information assets will consume limited organizational resources. They therefore should be treated by an organization as an item of value with the expectation of returning a favourable future return (e.g. prevention of theft of sensitive information).

As described in ISO/IEC 27004,[4] an organization needs to continuously evaluate and measure whether the applied information security has achieved its intended purpose. This measurement process equally applies to the assessment of the economic investment made by the organization in its limited goods and services. For example, are the costs of the following activities reasonable:

a) Cost of risk assessing processes and projects.

b) Organizational infrastructure, including the cost of people required to maintain information security .

c) Information security controls (e.g. cost of user access management solutions, cost of encrypting backups) providing adequate ongoing protection in accordance with the organization's risk appetite (e.g. accepted residual risk).

d) Activities to provide ongoing control testing, process assurance and/or certification to demonstrate the that information security has reached a specific standard.

e) Cultural development, training and awareness leading to a reduction in the number of information security related incidents.

NOTE Investments in organizational infrastructure and training can have slower but long-term effects on the organization. Their assessment should therefore be considered over a longer period of time.

7 Economic Objectives

7.1 Introduction

The application of economics to information security management requires appropriate data from the information security management programme to be used as input factors in any economic decision-making tools used by the organization. This process is straightforward for financial economic considerations, but more difficult for non-financial consideration.

Economic decisions involve the prioritization of available limited goods and service resources to optimize the achievement of organizational objectives. These economic decisions apply equally to information security management as to other parts of the organization.

Annex B provides examples of information security specific decision factors for consideration when optimising the achievement of multiple objectives. Each cost decision has the potential to influence the achievement of information security outcomes. For example, increasing investment in risk mitigation would allow the organization to operate at lower risk, but may not improve the organization's responsiveness to change.

7.2 Information Asset Valuations

Information asset valuations for information security purposes should be performed against the criteria of Confidentiality, Integrity and Availability (and any additional information security aspects

required by the organization). When establishing a value in monetary terms this value should reflect the business impact value of the asset if the actual criterion is compromised. For example, if a public website is compromised in terms of integrity (meaning that the information on that website is misleading), this may incur a certain business impact which could be expressed in monetary terms. The confidentiality value in monetary terms on the same website is zero as the information is publicly available. If the same website becomes unavailable, the business impact will have a different impact in monetary terms due to external parties not being able to access the information. Thus there exists three different values for this asset. This guidance should be considered when conducting asset valuations.

Since evaluation of intangible assets can be difficult, there are two simple approaches that could be adopted through the use of a simple comparative scale e.g. low, medium, high or a numerical scale such as 1-4 . This is especially suitable when values and/or costs are calculated and/or presented as a range of values (max, min).

Economic values that may be used as an economic justification relating to tangible and intangible assets for information security investment are categorised in Table 2.

Table 2 — Types of Organizational Economic Values

Value type	Description
Physical	Sum of the tangible assets that comprise an organization
Customer	Valuation of the business generated by the portfolio of clients of the organization
Societal	Valuation of the perception that society in general has of the organization
Reputational	Valuation of the perception that competitors, suppliers, customers, shareholders, governments and other stakeholder components have of the organization
Intangible / Logical	Sum of the intangible assets that comprise an organization. Intangible assets should also include the information handled by an organization: strategic, business, etc.
Legal and Regulatory	Potential sanctions and/or penalties that might result from a breach

The basic value model should be used in conjunction with the balance sheet for evaluating and presenting conclusions of information security economics and is based on the following characteristics:

Direct values are direct economic values, such as material loss, or direct investments based on an occurrence that can be passive or active. In this area the values can be precise.

Indirect values are extensions to the direct values and reflect the additional and more intangible values lost or gained. The indirect values have a greater uncertainty and as such they can be within a range. These values could include the value of lost output, increased administration, etc.

Extended values are those affected by the direct and indirect values and can be quite substantial. The extended values have a greater range and have to be evaluated based on the same basis as direct and indirect values, but will be affected by other factors as well such as impact on the society and/or the organization as a whole. This could include others such as share price if relevant, etc. Extended values here are often considered as unquantifiable values such as brand, reputation, etc. (Note extended values are most likely to be negative but may also be positive.)

An organization should complete its valuation of its information assets by considering the different stakeholders which include:

a) Tangible assets that comprise an organization.

b) Value of business generated by the portfolio of clients.

c) Intangible assets like information, customer perception, brand value, societal perception.

Table 3 — Types of Economic Asset Values - Principles and examples

Category	Value type	Description	Asset	Value
A	Organization	The parties within scope of ISMS.	The assets defined to be able to run and maintain the business over time.	The total value could be broken down to business processes related to specific assets such as intellectual property rights, databases, ICT resources, etc. to which values could be applied.
B	2nd and 3rd Parties	Individual customers, suppliers.	The assets defined to be able to run and maintain the business in relation to a defined party.	The value defined for the assets involved.
C	Stakeholders	Any party intertested in the information security aspects of the organization, such as owners.	The assets defined to be able to run and maintain the business in relation to a defined party.	The total value could be broken down to business processes related to specific assets such as IPR, Databases, ICT resources, etc. to which values could be applied.
D	Societal	Community interests.	Assets that could compromise the community interest.	Value of the impact on the community which is then transfered to the organization.

This valuation can also be graded so as to apply an appropriate combination of the relevant categories. For example, information assets associated with an entire database of 100,000 customer records containing personally identifiable information could be much more valuable when all organizational (category A), stakeholder (category C) and other affected party (category B) interests are aggregated.

Valuations may also be graded based on categories of important assets. For example, a database of 100,000 customer records containing personally identifiable information would be very important to a government department. Similarly, unpublished final accounts of a major international company would be very sensitive, with dangers of insider trading and major international economic repercussions.

Organizations can make informed economic decisions by mapping the relationship between cost decisions and the relative consequences. As each cost decision (e.g. on risk mitigation costs, on certification costs) can have multiple consequences, it may be possible to represent this relationship in a table.

8 Balancing Information Security Economics for ISM

8.1 Introduction

A well-functioning organization needs an information security management system that ensures its information assets remain protected from adverse events, while at the same time being available to those who need to use such information for sustainable organizational delivery of its business objectives. The common requirements associated with determining benefits and costs to be achieved by an organization to meet its business objectives are typically associated with:

a) Reduction of losses (often annualized).

b) Minimizing the costs associated with making financial and other provisions for loss events (incidents).

c) Effectiveness of the information security management programme designed to protect information assets.

d) Efficiency of the information security programme associated with the cost of planning, designing, implementing, maintaining and improving the programme.

Information security management can create intangible/non-financial and tangible/financial benefits with positive values when management maintains an ability to direct and control information security risks.

Cost and benefit decisions should relate to the expected benefits from achieving a risk reduction by the deployment of planned controls. Typically risks are mitigated by a number of controls. The deployment of a particular control may contribute at different levels to risk mitigation, ranging from a minor contribution through to full risk mitigation.

Information security should support the achievement of business objectives. It should be remembered that different approaches can be adopted, with different costs and benefits that will allow the desired business objectives to be achieved. For example, it may be possible to trade-off 'speed to market' benefits (e.g. increased revenue sooner) with increased 'potential information security loss' costs (e.g. privacy of new customer data not protected and accessed by unauthorised persons). In this case potential loss represents a valuation of the loss that could be incurred in absence or compromise of the information asset (customer data). Alternatively, it may be better to accept a higher cost Information security management programme to realize the benefits that would accompany good customer acceptance of a product or service.

8.2 Economic Benefits

A reduction in losses can be determined by comparing an anticipated annual loss in the absence and presence of the Information security management programme under consideration. When performing this comparison, consideration needs to be given to using a methodology that can be aligned with other methodologies in use by the organization.

Where different criteria or assessment techniques are used for determining information security risk, the overall economic results will most likely not be consistent and comparable with other programmes and initiatives. Similarly, to ensure a consistent and comparable outcome the risk criteria used to determine economic benefits should be restricted to those that have a financial focus. However, the organization should also consider how non-financial economic factors could be applied once the financial economic focus has been completed. Information about management of information security risks can be found in ISO/IEC 27005.[5]

It is important to note that the selection of the risk criteria relevant to determining financial economic benefits rarely resides with the information security management function and is often determined by the Chief Financial Officer or someone with a similar financial role.

Costs associated with minimizing financial loss and other provisions for loss events may be reduced as a consequence of an Information security management programme. This is an economic benefit that can be taken into account when evaluating a proposed Information security management programme.

8.3 Economic Costs

Costs of an Information security management programme to support particular business objectives should cover the entire lifecycle of the programme using a risk-based approach. Areas to be covered may include:

a) Planning.

b) Implementation.

c) Operation.

d) Maintenance.

e) Improvement.

f) Decommissioning.

Reporting and assurance procedures (including any auditing by customers, 3rd parties internal auditing or other assurance approaches) should also be included in the costs. Similarly, costs associated with training and maintaining awareness of people operating or using information security controls should be included in the costs.

Costs should also cover the entire information security management programme (see ISO/IEC 27001[1]) and should be associated with a measurement of all the anticipated benefits, not just the economic benefits (see ISO/IEC 27004[4]). This approach should be taken as it is often unrealistic to separate costs into categories associated with economic benefits and other benefits.

Maintaining knowledge about the costs and the effectiveness of the Information security management programme provides an additional benefit that would enable the organization to convey confidence and trust to organizational stakeholders.

Key cost areas should be considered when assessing the Information security management programme as shown in Table 4.

Table 4 — Key cost areas

Cost Area	Description
Risk assessment	Includes all costs related to risk identification, analysis and evaluation.
Training and awareness	Includes induction training, company wide programmes, targeted training, training assessment, reviews, training material development, presenters, and monitoring tools.
Controls	Includes direct costs for selecting and implementing controls to reduce risks, operating controls, other risk treatment options, and indirect costs related to organizational effectiveness impact related to control. Controls may be preventive, detective and/or reactive.
Certification	Includes costs related to control monitoring and testing, assurance functions, certification testing and anything that works towards validating the effectiveness of security controls. Certification costs are measured based on staff costs (performing control testing), cost of audits, and cost of maintaining certifications or registrations with authorized bodies.
Audit	Includes cost for audit resources (external and/or internal) and should include internal staff time costs for the audit as well as planning, supporting and follow-up.
Measurements	Includes costs for external and/or internal sourcing for measurement programmes, tools and their application and should include internal staff time costs for providing the measurement results.

8.4 Applying Economic Calculations to ISM

8.4.1 Overview

To achieve objectives for information security a business case has to be presented that includes information security economics based on a calculation model, see Annex C.

An economic business rationale for information security investments should include costs, revenues and returns, i.e. the business rationale for accepting the costs and investments involved.

As any case will be unique, a case specific approach should be considered. Information security economics is not very different to economics used to justify investments designed to use marketing to create a sales impact. The benefit in terms of revenues and returns are very seldom known and have to be estimated.

The business cases can be categorized into two types as described in 6.2. The application of models to a case can be seen as a hierarchy as shown in Figure 2. The method can be applied in several layers and if suitable, aggregated. Aggregation is easier to use in a category B business case as this has a more limited scope.

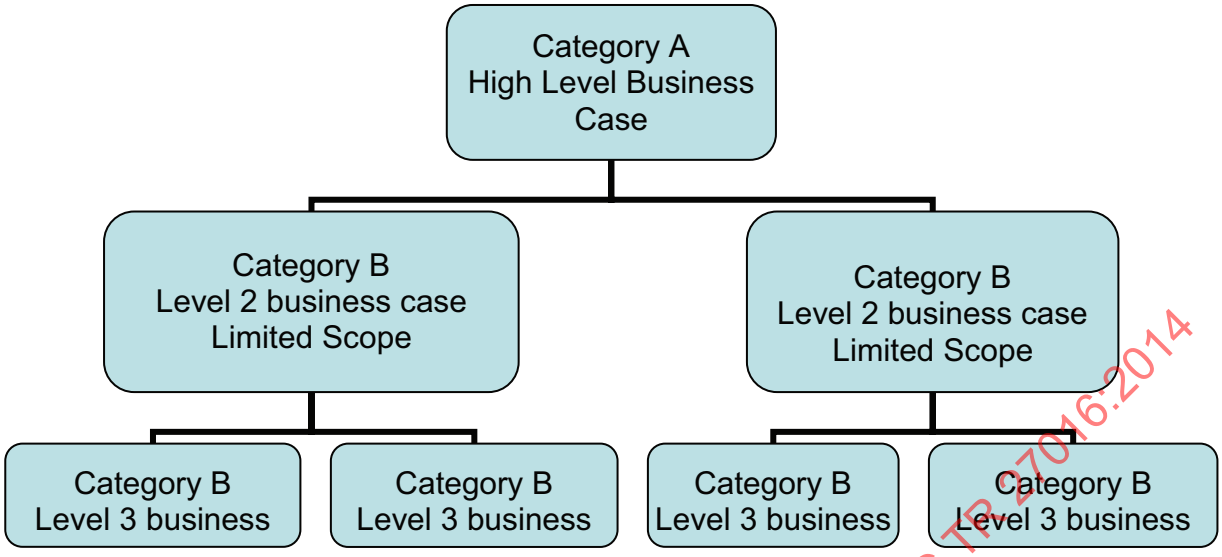

Figure 2 — 'Bottom up' approach to compiling an Information Security Management business case

The biggest difference when applying an economic model is that the organizational wide category (A) is often applied "Top-Down", while the partial category (B) has a more narrow scope applied "Bottom-Up".

A model for the organizational wide category (A) could be supported by a more detailed model(s) if accurate data are available. When applying the organizational wide model (A) or the partial model (B), the accuracy of the calculation will be affected by:

a) Availability of existing information related to the economics calculation such as value of assets, statistics, etc.

b) Available resources for the results such as time, people, finance, etc.

c) Availablity of business knowledge such as expertise, internal or external.

A simplistic approach can use categorization as the starting point and then evolve the economics calculation based on the initial calculation.

8.4.2 Guidance

The following steps should be taken as part of ISM in order to identify the business rationale and use an economic method, referred to as "the case":

a) Establish Context

   1) Get business based description if available.

   2) Establish the scope of the case.

   3) Establish the context of the case.

   4) Establish the stake holders.

   5) Establish who should make the business decision on the case.

   6) Determine the category of the case.

b) Define assets that are affected by information security within the scope of the case such as:

   1) Critical information.

2) ICT system.

3) Any other assets defined.

4) The assets' information security value which should be listed for the assets defined.

5) The basic approach to be used for calculations including models and aggregation.

c) Determine objectives of the case.

1) Description in qualitative terms.

2) Description in quantitative terms.

3) Conclude in monetary terms.

d) Determine time.

1) How long is the case expected to have an impact on the organization:

i) Long term cases - more than one year, and if so, how many years.

ii) Short term – maximum one year.

e) Define costs for applying the case such as:

1) Short term costs (not to be used for more than a year and will have no impact on the organization after that).

2) Investment costs (one time costs but will have an effect during the case).

3) Running costs – annual costs for the case during its time.

4) It is useful to consider costs as direct costs, indirect costs or extended costs (see also model C.3).

f) Define benefits and value of the case such as:

1) Compliance benefits by avoiding penalties.

2) Compliance/sales opportunities by attracting new markets.

3) Image/sales opportunities by attracting new markets.

4) The positive value of risk reduction.

5) The value of increased internal efficiency.

6) The information security value of each asset if compromised.

7) Any other comparable case.

8) For value the concept of turning negative cost into opportunity value can be used (see also Annex C).

g) Use possible interaction between cost and value

All the above may be applicable but often the context of the case means that only some of the values apply. Information on values may also come from different,but related sources. For example, risk reduction value may also include compliance penalties. The information security value is often also a reflection of consequences related to risk. In practical terms many sources may be used.

Finalize the basis for selecting method.

1) If context and scope are organization wide, a method such as BVM and/or a generic investment calculation may be appropriate. A combination of the two would not be unusual(ref. Category A business case).

2) If context and scope are narrow and asset/control focused, a method such as ROI could be used (ref. Category B business case).

3) If the context and scope are a combination of the above, both methods above could apply, but there may need to be consideration of assetsand their CIA impacts (ref. Category B business case).

8.4.3 A Business Case Based on an Organization-Wide Approach(Category A)

A wider context case (Category A) could be applied through economic values being either broken down in detail and then aggregated (Bottom-Up) or identified using an overview analysis method (Top-Down) where details are estimated. The latter method is likely to contain a lot of uncertainty which may make it invalid, while giving an impression of being precise for management making the decision on the case. It will also be quite time consuming without providing the intended quantitative results.

The method can be implemented in stages . The method is generally an iterative process with inputs changing as information is gathered and therefore changes are being made before a final calculation is made. It is often easier to identify a range of input values or results than precise values. Where a range can be used, it might be useful to document likely maximum and minimum values.

Input Positive:

a) Direct annual opportunity value, such as incident cost reduction.

b) Indirect opportunity value applied over the time of the case, such as avoiding penalties through compliance.

c) Extended opportunity value applied over the time of the case, such as sales opportunities for new market.

Input Negative:

d) 1. Direct annual costs, such as running costs.

e) 2. Indirect cost applied over the time of the case, such as setting up a project.

f) 3. Extended cost applied over the time of the case, such as sales loss.

See D.1 for an example (using the model mentioned in C.2 and C.5).

This could also be calculated from the assets within the scope (“Bottom-Up”) using the principle in table two. This approach will be more accurate but is extensive work and depends on assets being defined; in many instances this is not easily available. This refers to the “Bottom – Up” approach based on Figure 2.

8.4.4 A Business Case Based on a Part of the Organization (Category B)

A partial context case (Category B) means that all economic values have to be gathered at a detailed level, and then aggregated (“Bottom-Up”).

The complexity of a partial category (Category B) case may vary greatly. Models D.2 and D.3 show a narrow scope application and then a broader one.

The method can be applied in stages. It is generally an iterative process with inputs changing as information is gathered. A final calculation cannot be made until all the changes are complete. It is often easier to identify a range of input values or results than precise values. Where a range can be used, it might be useful to document likely maximum and minimum values.

Input Positive:

a) CIA value of the asset/assets within the scope of the business case.

b) Define the impact on the value taking account of CIA risk.

c) Turn the negative impact to an opportunity value assuming correct information security levels for each of the confidentiality, integrity and availability scenarios (i.e. none of the risks identified materialise).

Input Negative:

d) Direct annual costs, such as running costs for mitigating the risk.

e) Any indirect cost applied over the time of the business case, such as setting up a project.

f) Extended cost applied over the time of the case, such as sales loss.

See D.2 for example.

A partial context business case (category B) that is very limited in scope means that all economic values have to be gathered at a detailed level, which could then be directly applied to the case.

Construct a short analysis and select a simple method such as the negative to positive model which can be rapidly conducted and understood (refer to C.5).

Input Positive:

a) Estimate actual or potential business impact related to information security.

b) Estimate the positive value for the activity of the business case.

c) Conclude if there are any other positive values that may occur depending on the activity and decide if to include them or not. This will depend on the case and the information available.

Input Negative:

d) Define the direct and indirect control(s) required to mitigate the impact.

e) Define the direct and indirect costs for applying the control(s).

Conclude:

f) Establish the net value/costs.

g) Compare and decide.

See D.3.

Annex A
(informative)

Identification of Stakeholders and Objectives for Setting Values

A.1 Overview

The purpose of this annex is to assist organizations in understanding the wider economic impact of their information security management programmes and related investments. There are a variety of constituencies that could benefit from an organization's improved information security management.

The nature and size of the economic benefit will depend on how organizations leverage the benefits they can achieve associated with more efficient information security management.

A.2 Critical Public or Private Sectors

Public and private sector organizations in industry sectors in which information security is a primary business objective (such as banking, government, health and defence) clearly depend on establishing and maintaining information security as a core part of their brand value and image, and indeed is an inherent part of their products and services. By the same token, if organizations in such sectors suffer information security incidents, their brands may be harmed and, in the worst cases, they may be put out of business.

A.3 Public Health and Safety

The proposed standard does not explicitly affect public health and safety. However, it will indirectly affect the safety of many forms of medical treatment by ensuring that the information on which such treatment is based receives adequate security protection.

A.4 Societal and Community

The proposed standard is broadly applicable to organizations that operate and deal with all sectors of society. It is unlikely to have an adverse impact on minority or disadvantaged groups and will in fact benefit all stakeholders as well as society and the community generally.

A.5 Personal Information

In cases where information concerns individuals and their privacy, the standard will have a beneficial effect because it is likely that the protection of personal and sensitive information will be improved in organizations that use this standard in association with an information security management system.

For most organizations the management of the vast stores of personal information is one of the areas where greater information security challenges are encountered. A compromise of the security of personal information could result in negative externalities.

A.6 Environmental

The proposed standard will not directly impact the environment to any significant extent.

Indirectly the proposed standard will have a positive effect on the environment because it is likely that information critical to effective environmental management will receive better protection in

organizations that use it in association with an information security management system that may currently be the practice.

A.7 Competition

Organizations that make good use of information security may achieve a competitive advantage over those that do not because related risks are better managed.

Annex B
(informative)

Economic Decisions and Key Cost Decision Factors

Ref	BUSINESS OBJECTIVES	COST DECISIONS			
		Risk Mitigation Costs	Certification Costs	Risk Management Organizational Costs	Control Costs
A	Enabling the business to participate in high risk endeavours, by increasing risk management maturity and operating at lower risk than competitors	Yes Systems with lower risk will allow participation in a high risk environment	Yes. Business partners may be influenced to participate based on demonstrable security certification	Yes Business partners are more likely to partake in higher risk ventures if the organization can demonstrate a more mature risk organization	Yes Controls applied are generally a wide set of controls that affect the whole business such as training. Cost for each control is dependent on the controls themselves and the information security maturity of the organization
B	Enabling the business to satisfy regulatory requirements thereby avoiding operational resource limitations and penalties, e.g. by improving compliance	Yes Organizations with better risk mitigation have better regulatory positions	Maybe Certification may directly contribute to satisfying regulatory requirements	No Increasing expenditure on risk management organization does not directly result in an improved regulatory position	Yes Controls applied are generally a wide set of controls that affect the whole business as well as specific technical controls. The cost of each control depends on the controls themselves and the information security maturity of the organization
C	Enabling the business to be versatile, agile and responsive to change, e.g. by building flexibility into security solutions	No Mitigating risks do not necessarily make an organization more agile	No Certification does not improve an organization's agility	Yes Increasing expenditure on operational risk organization is more likely to enable a business to manage higher risk opportunities effectively	No Controls genereally do not contribute to organizational agility. This has more to do with ISM and the maturity of the ISMS
D	Achieving an acceptable level of predicted (future) loss, based on the expected risk profile, e.g. by mitigating risks based on risk value (ALE)	Yes Risk mitigation directly drives expected loss levels	No Certification does not directly drive lower risk and expected loss rates	Yes Increasing expenditure on operational risk organization is more likely to reduce risks and expected losses	Yes Controls can be applied directly to mitigate risks
E	The annualized loss expectancy (ALE) expresses the product of expectance values (mean values) of loss as well as of occurrence. Such a calculation of risk level does not provide sufficient results for "low frequency / large impact incident(s)". Information security controls should also cover these "low frequency / high impact incidents" as they are a real information security concern . The calculation of a Value-at-risk (VAR) has the potential to deliver better results than the ALE.	Yes Risk mitigation directly drives expected loss levels	No Certification does not directly drive lower risk and expected loss rates	Yes Increasing expenditure on operational risk organization is more likely to reduce risks and expected losses	Yes Controls can be applied directly to mitigate risks

Ref	BUSINESS OBJECTIVES	COST DECISIONS			
		Risk Mitigation Costs	Certification Costs	Risk Management Organizational Costs	Control Costs
F	The annualized loss expectancy (ALE) expresses the product of expectance values (mean values) of losses as well as of occurrence. Such a calculation of risk level does not provide sufficient results for "very low frequency / very large impact incidents" at all. However, information security controls should also cover these "very low frequency / very high impact incidents". The calculation of an average expected loss has the potential to deliver better results than the ALE.	Yes Risk mitigation directly drives expected loss levels	No Certification does not directly drive lower risk and expected loss rates	Yes Increasing expenditure on operational risk organization is more likely to reduce risks and expected losses	Yes Controls can be applied directly to mitigate risks
G	Maintaining reputation and share price by enabling the business to differentiate on "trust", e.g. by certifying to standards and mitigating high impact risks that are more likely to impact reputation if they occur	Yes Risks likely to cause reputational impacts can be mitigated	Yes Certification can improve reputation	Yes Increasing expenditure on operational risk organization can improve reputation, especially to prospective employees	No Controls directly do not contribute to maintaining share price. This has more to do with ISM and the maturity of the ISMS
H	Minimising expected operational costs of operating information security and risk management, e.g. by improving efficiency	No Mitigating risks may not cause operations to be more efficient	No Certification is not expected to lower operational costs	No Increasing the amount spent on risk management is not expected to improve efficiency directly	No Controls directly do not contribute to improving efficiency related to risk management. This has more to do with ISM and the maturity of the ISMS including awareness, measurements, audits, etc.
I	Providing assurance on the completeness and accuracy of risk information and governance reporting	Yes Increased investment in assurance is likely to identify ineffective risk treatment, driving subsequent improvement	Yes Certification provides some increase in process assurance	Yes Increasing head count will allow increased assurance functionality	No Controls directly do not contribute to risk and governance. This has more to do with ISM and the maturity of the ISMS including awareness, measurements, audits, etc.
J	Protecting staff from personal liability, e.g. performing due diligence to avoid directors' liability	Yes Directors could be negligent if investment in risk mitigation was inadequate	Yes Directors may be able to demonstrate due diligence by gaining external certification	Yes Directors may be negligent if investment in risk management is inadequate	Yes Controls of roles and responsibility for information security.
K	Meeting community expectations as an infrastructure and service provider, by protecting their information	Yes Risks to customer information can be mitigated	Yes Certification can be used to improve protection of customer information	No Increasing expenditure on risk management does not directly result in improved protection of customer information	No Controls directly do not contribute to community expectations. This has more to do with ISM and the maturity of the ISMS including awareness, measurements, audits, etc. to provide feedback to the community
L	Providing employment opportunities to the community	Yes Spending on risk mitigation provides employment opportunities for those doing the mitigating	No Certification does not directly result in employment opportunities	Yes Increasing expenditure on risk management organization creates more employment opportunities	No Controls directly do not contribute to employment opportunities. This has more to do with ISM and the maturity of the ISMS including awareness, measurements, audits, etc..

Ref	BUSINESS OBJECTIVES	COST DECISIONS			
		Risk Mitigation Costs	Certification Costs	Risk Management Organizational Costs	Control Costs
M	Avoiding requirements for risk and audit capital and additional oversight burdens by operating within acceptable parameters	Yes Mitigating risks is the key means of avoiding risk and audit capital	No Certification is unlikely to lead directly to reduction in risk and audit capital allocation	No Increasing expenditure on the risk management organization does not lead directly to reduction in risk and audit capital	No Controls do not directly avoid risk and audit capital allocation (unless those controls are deficient)
N	Avoiding impacts on external parties such as infrastructure and service providers	Yes Mitigation of risks is likely to reduce the risk of impacts on external parties, infrastructure and service providers	No Certification does not directly result in reduction of impacts to external parties	No Increasing expenditure on risk management organization does not lead directly to reduction in risk to external parties	Yes Controls may directly avoid impacts
O	Systems to manage and disseminate security policies, procedures, etc.	Yes Likely to reduce the risks of human errors	Yes Part of certification audit scope and will contribute	No There is no increase in risk management organization costs	No Controls directly do not contribute to learning. This has more to do with ISM and the maturity of the ISMS including awareness, measurements, audits, etc.
P	Identity/authentication and access management systems to control user IDs, access rights/permissions, etc. for application systems	Yes Likely to reduce the risks of loss of confidentialty and integrity and may increase handling costs as well as costs of technical solutions	No Maybe part of certification audit scope	No There is no increase in risk management organization costs	Yes The controls related to this subject apply
Q	Vulnerability and change management systems to help keep up to date with security patches	Yes Likely to reduce the risks of loss of Confidentialty and Integrity. May increase handling costs as well as costs of technical solutions	No Maybe part of certification audit scope	No There is no increase in risk management organization costs	Yes The controls related to this subject apply
R	Incidents with an estimated value sufficent to justify ISMS generation which will lead to overall savings. Provided estimates are sufficiently conservative and rational to survive management challenge, reduced incident costs alone will typically be more than sufficient to justify the cost of the ISMS even though they do not constitute the whole business case	Yes If incidents are added to risk processes this will increase the complexity but also provide more accurate evaluations	No Maybe part of certification audit scope	Yes May increase risk management organization cost	Yes The controls related to this subject apply
S	Addressing information security risks and controls for market, legal or regulatory reasons	Yes But this should be a major part of risk handling	Yes Part of certification	Yes May increase risk organization	Yes Compliance controls apply

Annex C
(informative)

Economic Models Appropriate for Information Security

C.1 General information

There are many calculation models that apply to economics. In terms of information security these as well as others could be used. Only very generic models are listed in this annex.

The precise economic implications of implementing information security processes, procedures or technical measures may be difficult to identify. It is therefore recommended that results of calculations be presented within ranges using likely maximum and minimum values. This is not covered in the models as this is done by using one model but with different values and/or costs.

C.2 Basic Value Model (BVM)

The principle basic value model 1 applies both for positive (yield) and negative (costs) values and should be used in conjunction with the negative to positive and the balance sheet that is presented in the table for a complete set of method steps for evaluating and presenting results.

The principle of BVM 1 is based upon three areas with different characteristics as below:

Direct values cover direct economic values, such as material loss, or direct investments based on an occurrence that can be passive or active. In this area the values can be more precise.

Indirect values are extensions to the direct values and reflect the additional and more intangible values lost or gained. The indirect values have a greater uncertainty and as such they can be within ranges. They could be an evaluation of values such as lost output, increased administration, etc.

Extended values are those affected by the direct and indirect values and can be quite substantial. Extended values have a greater range and have to be calculated using the same basis as direct and indirect values, but will also be affected by other factors such as impact on society and/or the organization as a whole, or share price if relevant, etc. Extended values of items such as brand, reputation, etc. are often considered to be difficult to quantify. (Note extended values are most likely to be negative but may also be positive as a consequence when information security is applied.)

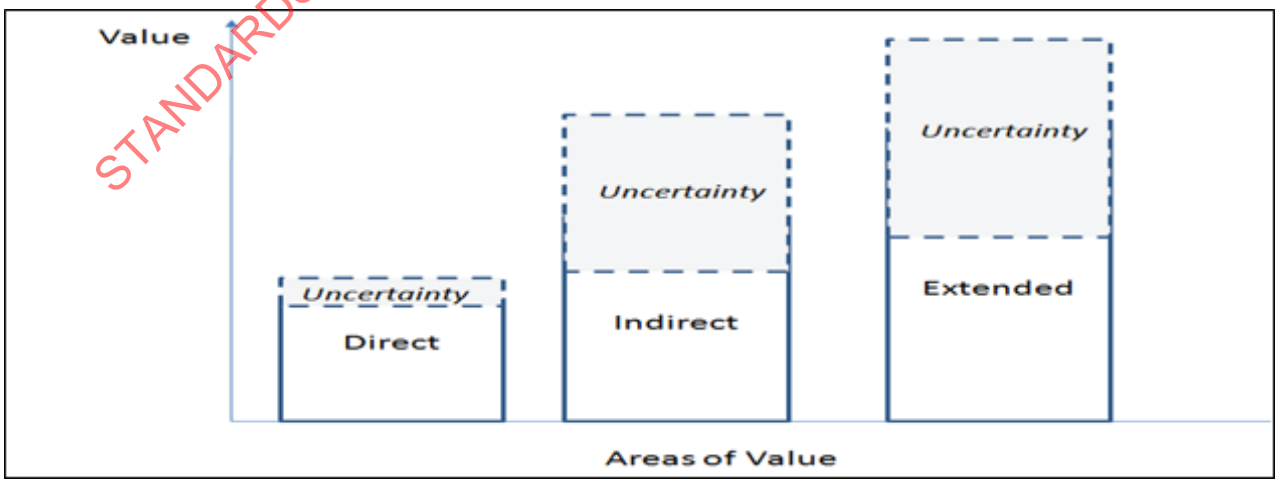

Figure C.1 — Principle basic value model

C.3 Negative to Positive Model

An approach to turning negative values* to positive values* is based on the alternative questions:

— What will the negative value be if an activity is not done?

— What will the positive value be if an activity is not done?

— What will the negative value be if an activity is done?

— What will the positive value be if an activity is done?

Note - Values used in the model as costs can be positive

Answering these questions in combination with the principle Basic Value Model, Figure C.1 will then create a balance board with four squares as shown in Figure C.2.

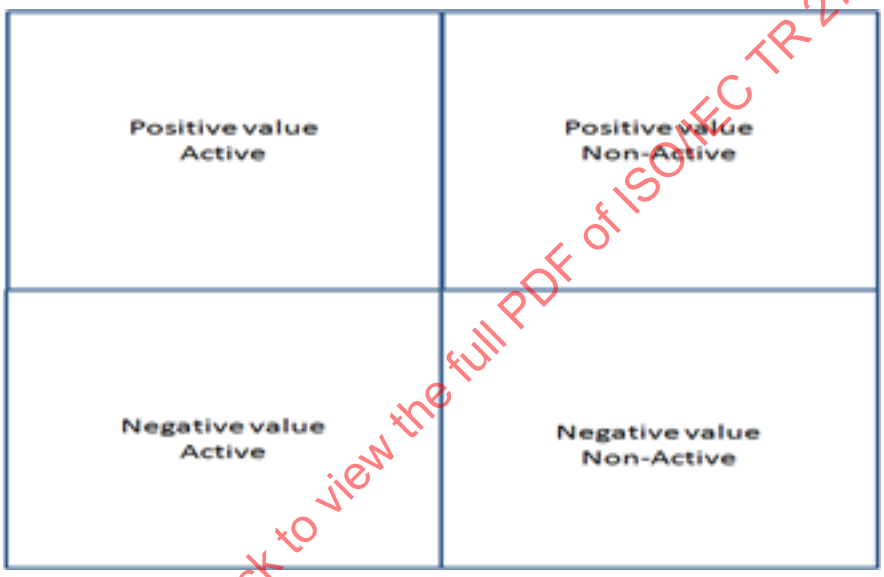

Figure C.2 — Negative to Positive model

The use of the model will ensure that all aspects will be covered. However there are also duplications of values related to the same activity. This can be handled by using a simple balance table as seen in Table C.1 below.

Referring to Table C.1, in some cases the amount in A1 is the same as in D2 and thus the negative value/cost can be turned into a positive value when comparing the net for the two rows (1 and 2).

(If an activity is complex, further rows can be used but then the summary should still be between current state (the possible activity not done) and when the activity is fully implemented/done.)

Table C.1 — Balance table for net values

	Base	Activity	Positive value activity done	Positive value activity not done	Negative value activity done	Negative value activity not done	Net
Ref			A	B	C	D	
1	**A possible activity to change the current situation**	Activity "X" done	*Value*	Not applicable	*Cost*	Not applicable	*1A-1B*
2	**The possible activity not done**	Activity "X" not done	Not applicable	*Value*	Not applicable	*Cost*	*2B-2D*
NOTE The table shows the principle and can be further simplified by deleting the cells that are not applicable.							

C.4 Generic Balance Investment for Protection Cost vs. Value Theory

The theory is that an optimum balance point can be reached by applying gradual protection costs to value. The optimum point between the protection and value costs is when the reduction of risk that will affect the value will be less than the cost of protection. The basic factors for the theory are:

a) The knowledge of value (which is constant)

b) The known cost of protection (which will increase depending on actions)

c) The reduction of risk in relation to applying protection (which is based on the value and how effective the protection is)

The value and costs for protection can often be established but the reduction of risk is often an estimate.

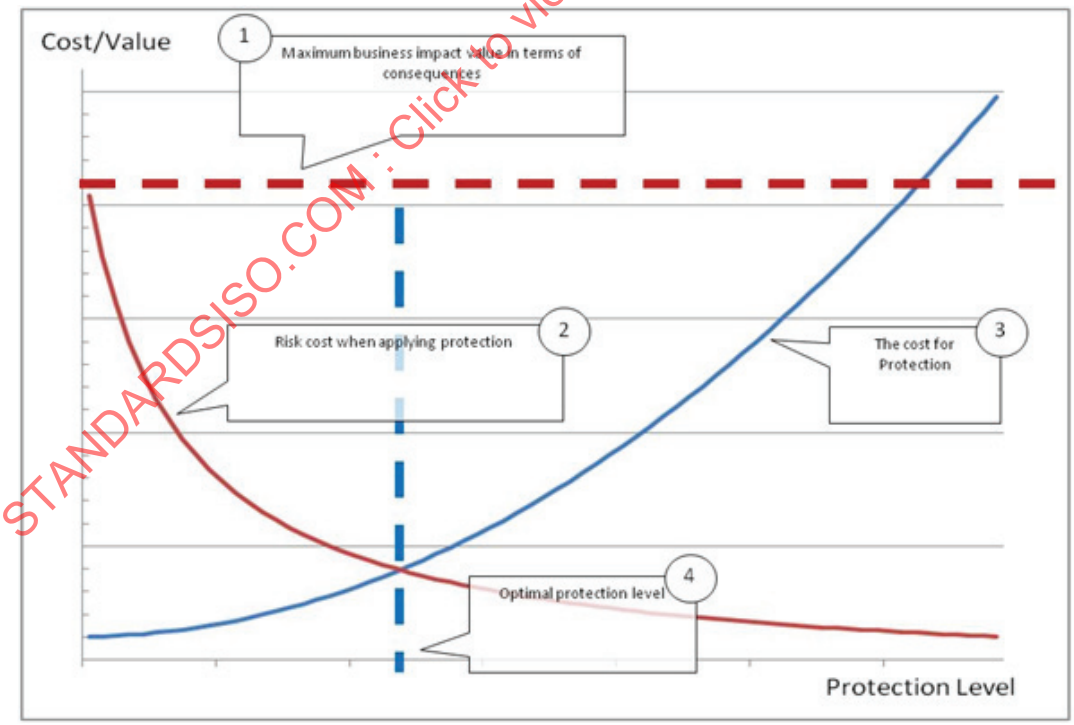

Figure C.3 — Optimum Balance Theory between Protection Cost and Value