DRAFT ISO/IEC GUIDE 81

Secretariat: **TMB**

Voting begins on 2009-12-04

Voting terminates on 2010-04-04

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION

Guidelines for the inclusion of security aspects in standards

Lignes directrices pour l'inclusion des aspects de sécurité dans les normes

ICS 01.120

To expedite distribution, this document is circulated as received from the committee secretariat. ISO Central Secretariat work of editing and text composition will be undertaken at publication stage.

Pour accélérer la distribution, le présent document est distribué tel qu'il est parvenu du secrétariat du comité. Le travail de rédaction et de composition de texte sera effectué au Secrétariat central de l'ISO au stade de publication.

In accordance with the ISO/IEC Directives, Part 1, 2008, clause A.5, this draft Guide is submitted to the ISO and IEC national bodies for approval. Ballot papers should be returned to the ISO Central Secretariat by the date shown above.

Contents

Page

Foreword ... iv

0 Introduction ... v
0.1 The concept of security ... v
0.2 Security of products ... v
0.3 Security of processes and systems: ... vi

1 Scope ... 1

2 Terms and definitions ... 1

3 Inclusion of security aspects in standards ... 5
3.1 General ... 5
3.2 Assessing security risks ... 5
3.3 Determining tolerable risk and risk reduction ... 6
3.4 Achieving tolerable risk ... 6

4 Security aspects in standards ... 8
4.1 Coordination ... 8
4.2 Analysis of standards ... 8
4.3 Preparatory work ... 9
4.4 Security of products ... 9
4.4.1 General ... 9
4.4.2 Security aspects with respect to product packaging ... 10
4.4.3 Security aspects to be considered during testing ... 10
4.5 Security of processes: ... 10
4.6 Security of systems: ... 10

5 Drafting ... 11
5.1 General ... 11
5.2 Information on security aspects ... 11
5.2.1 Type of information ... 11
5.2.2 Instructions ... 11
5.2.3 Warning notices ... 12

Bibliography ... 13

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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

Draft Guides adopted by the responsible Committee or Group are circulated to the member bodies for voting. Publication as a Guide requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

The ISO/IEC Guide was prepared by the Strategic Advisory Group on Security

0 Introduction

0.1 The concept of security

Consideration of security aspects in new and existing standards can contribute to increased security and protection. Security is concerned with enabling and improving the capability of public and private stakeholders to prepare for and respond to a wide range of threats and hazards (natural, technological, and human – both unintentional and intentional), in an all hazards approach. This by its very nature requires that security both considers and integrates a range of interconnected disciplines including: asset protection (physical, environmental, financial, information and human), as well as risk management; crisis management; emergency management; business continuity management, and recovery management.

The increasing complexity of products, processes and services entering the market also requires that the consideration of security aspects be given a high priority. Inclusion of security aspects in standardization provides protection from and response to risks of unintentionally, intentionally, and naturally caused crises and disasters that disrupt and have consequences on societal assets.

0.2 Security of products

This Guide covers the consideration of security aspects in product standards. It is intended to promote the use of techniques for identifying and assessing the security aspects of technical provisions in standards, and for minimizing security risks and threats. Its purpose is:

a) to raise awareness that provisions in product standards can affect product security and integrity in both negative and positive ways;

b) to raise awareness that provisions in product standards should consider dual-use applications of products for conventional and security applications;

c) to raise awareness that provisions in product standards should consider the product's continuing utility in an emergency situation and operation in crisis and disaster situations;

d) to raise awareness that provisions in product standards should consider deliberate misuse of products, throughout their life cycle, to create a security risk;

e) to outline the relationship between product standards and security;

f) to help avoid provisions in standards that may lead to increased security risks;

g) to emphasize the balanced approach in standard development that is required to deal with competing priorities and issues such as **security**, product function and performance, health and **safety**, and other regulatory requirements;

h) to promote the regular review and revision of existing standards in the light of technical innovations, permitting improvement in the security aspects of products, processes, and services.

NOTE 1 It may be necessary to consider quality requirements in standards to ensure that the security requirements are consistently met.

NOTE 2 The term "standard" used throughout this Guide includes International Standards, Technical Specifications, Publicly Available Specifications and Guides.

NOTE 3 Although this Guide is intended primarily for use by standards writers, its underlying principles may be used wherever security aspects of standards are being considered.

NOTE 4 Standards may deal exclusively with security aspects or may include clauses specific to **security**.

NOTE 5 Unless otherwise stated, the term “committee(s)”, when used in this Guide, is meant to cover both ISO and IEC technical committees, subcommittees or working groups.

NOTE 6 Terms defined in clause 3 are printed in bold type throughout this Guide. (Not currently true.)

NOTE 7 **Safety** is dealt with in standards work in many different forms across a wide range of technologies and for most products, processes and services. (see ISO/IEC Guide 51). When including security aspects in standards writing, the concepts and considerations are similar to those presented in ISO/IEC Guide 51. However, security focuses on the protection of assets and the protection from disruption of functions, activities and operations of individual organizations, as well as society as a whole.

0.3 Security of processes and systems:

Prevention, including the avoidance, detection and deterrence of risks and threats to the security of processes and systems begins with the design processes and systems with the objective of protecting assets (human, physical or environmental) in the event of an emergency response. Consideration must also be given to recovery capability which is critical to ensuring operational continuity in the context of the following priorities:

— life safety;

— protection of assets;

— prevent further damage;

— reduce length of disruption;

— restore critical operations;

— recover to normal operations;

— protect image and reputation.

Guidelines for the inclusion of security aspects in standards

1 Scope

This Guide provides standards writers with guidelines for the inclusion of security aspects in standards. It is applicable to any standard related to the protection of assets, human, physical and or environmental, or a combination of these assets.

This Guide adopts a preventive approach aimed at reducing the **risk** arising from the use of products, processes or services. When security aspects are adequately considered in the development of standards, it furthers the objectives of promoting personal, public and environmental security, providing for protection and reducing the risk of damage or injury. It is intended for standards writers; however, this Guide also provides guidance of value to those involved in design work and other activities where security aspects are being considered.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

NOTE The use of the words secure and **security** as a descriptive adjective is avoided because the terms are not subject to a universally agreed upon or understood definition. As well, the term secure can be interpreted as an assurance of guaranteed freedom from **risk**. The approach in this Guide is to use the term **security aspects** to identify those characteristics, elements or properties which can be related to hazards, threats, vulnerabilities and impacts.

2.1
crisis
incident(s), human-caused or natural, that requires urgent attention and action to protect life, property, or environment

2.2
consequence
outcome of an event

NOTE 1 There can be more than one consequence from an event.

NOTE 2 Consequences can range from positive to negative.

NOTE 3 Consequences can be expressed qualitatively or quantitatively.

2.3
disaster
situation where widespread human, material, economic or environmental losses have occurred which exceeded the ability of the affected organization, community or society to come using its own resources.

2.4
dual use
products, processes, services and technology developed for conventional uses, but which can be used for security or military applications or to produce weapons of mass destruction

2.5
emergency
sudden, urgent, usually unexpected occurrence or event requiring immediate action. NOTE: An emergency is usually a disruptive event or condition that can often be anticipated or prepared for but seldom exactly foreseen.

2.6
event
occurrence or change of a particular set of circumstances

NOTE 1 Nature, **likelihood**, and **consequence** of an **event** can not be fully knowable.

NOTE 2 An event can be one or more occurrences, and can have several causes.

NOTE 3 **Likelihood** associated with the event can be determined.

NOTE 4 An event can consist of a non-occurrence of one or more circumstances.

NOTE 5 An event with a **consequence** is sometimes referred to as “incident”.

NOTE 6 An event where no loss occurs can also be referred to as a "near miss", "near hit", "close call" or "dangerous occurrence".

2.7
harm
physical injury or damage to the health of people, or damage to property, the community, or the environment

[ISO/IEC Guide 51]

2.8
hazard
potential source of harm

NOTE Hazard can be a source of risk.

2.9
hazardous situation
circumstance in which people, property or the environment are exposed to one or more **hazards, risks, or threats**

2.10
impact
evaluated consequence of a particular outcome

2.11
incident
event that might be, or could lead to, an operational interruption, disruption, loss, emergency or crisis

2.12
intended use
use of a product, process or service in accordance with information provided by the supplier

2.13
operational continuity
strategic and tactical capability, pre-approved by management, of an organization to plan for and respond to conditions, situations and events in order to continue operations at an acceptable predefined level

NOTE Operational continuity is the more general term for business continuity. It applies not only to for-profit companies, but organizations of all natures, such as non-governmental, public interest, and governmental organizations.

2.14
precautionary principle
response to uncertainty, in the face of risks to critical assets, health, property or the environment by acting to avoid serious or irreversible potential harm, despite lack of scientific certainty as to the likelihood, magnitude, or causation of that harm

2.15
preventive measures
means used to reduce risk

NOTE Preventive measures include risk reduction by inherently safe design, protective devices, personal protective equipment, information for use and installation, and training.

2.16
reasonably foreseeable misuse
use of a product (throughout its life cycle), a process or service in a way not intended by the supplier, but which can result from readily predictable human behaviour

2.17
residual risk
risk remaining after risk treatment

NOTE: 1 Residual risk can contain unidentified risk.

NOTE 2 Residual risk is also known as *retained risk*.

2.18
risk
effect of uncertainty on objectives

NOTE 1 An effect is a deviation from the expected - positive and/or negative.

NOTE 2 Objectives can have different aspects such as financial, health and safety, and environmental goals and can apply at different levels such as strategic, organization-wide, project, product, and process.

NOTE 3 Risk is often characterized by reference to potential events, consequences, or a combination of these and how they can affect the achievement of objectives.

NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event or a change in circumstances, and the associated likelihood of occurrence.

2.19
risk analysis
systematic process to identify **hazards and threats** and to estimate the **risk**

2.20
risk evaluation
process of comparing the estimated **risk** against given **risk criteria** to determine the significance of the **risk**

2.21
risk assessment
overall process of risk identification, **risk analysis** and **risk evaluation**

NOTE Risk assessment involves the process of identifying internal and external threats and vulnerabilities, identifying the likelihood of an event arising from such threats or vulnerabilities, defining critical functions necessary to continue the organization's operations, defining the controls in place necessary to reduce exposure, and evaluating the cost of such controls.