FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/FDIS
23234**

ISO/TC **59**

Secretariat: SN

Voting begins on:
2020-11-26

Voting terminates on:
2021-01-21

Buildings and civil engineering works — Security — Planning of security measures in the built environment

Bâtiments et ouvrages de génie civil — Sûreté — Planification des mesures de sûreté dans l'environnement bâti

Reference number
ISO/FDIS 23234:2020(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 59, *Buildings and civil engineering works*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

0.1 General

The objective of this document is to provide requirements and recommendations for organizations to effectively plan security measures in order to protect their built environment (e.g. buildings, plants, infrastructure, and property) against undesirable intentional actions.

This document describes an approach to planning security measures in the built environment based on generic stages and corresponding security deliverables in each stage. This document also defines a number of roles that should be assigned in the project organization to ensure that the security input to the design and construction process has been founded on professional assessment.

For practical use, the individual organization can adapt this document to its own project model and other organization-specific factors. This can also require that individual tasks be moved or allocated to other stages than those specified in this document.

This document is applicable independent from the chosen risk assessment methods, standards and guidelines for the project. Risk assessment methods are not described in this document and neither is the design of mitigation measures.

Figure 1 shows a checklist for when this document becomes applicable.

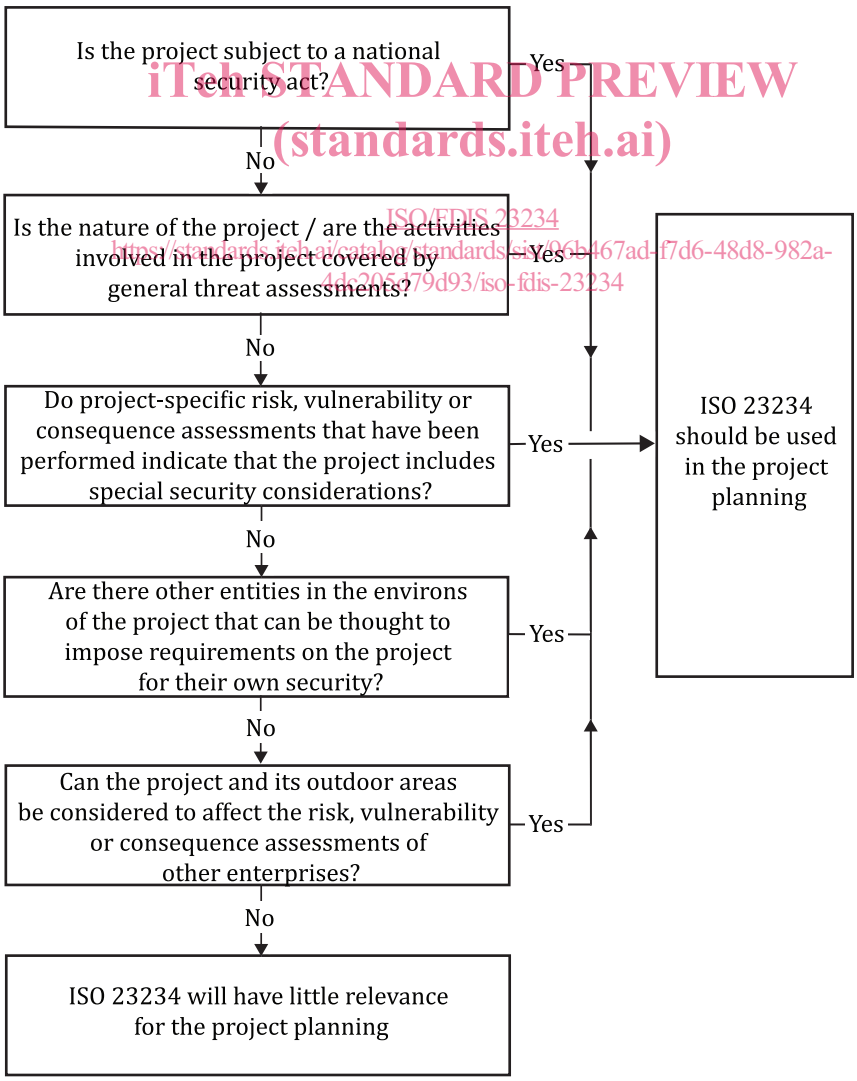

Figure 1 — Checklist as guidance for possible use of ISO 23234 in built environment projects

0.2 National security regulations

In addition to the requirements ensuing from the organization's own risk acceptance, organizations that are subject to national security regulations (where they exist) can be obliged by law to protect critical assets (material and functional).

For organizations not subject to such regulations, it is natural to base their approach on the insurance companies' requirements for their basic security. This document is general in nature and for general use, both within and outside of the scope of application of national security regulations.

0.3 Safety and security

This document is targeted primarily at the domain referred to as protective security. In this document the common word "safety" and the term "protective security" are used to distinguish between methods of combating undesirable unintentional incidents or accidents (safety) and combating undesirable intentional actions (protective security).

In the context of protective security, risk is usually understood as "an expression of the relationship between the threat against a specific asset and this asset's vulnerability to that specific threat". The threat derives from a threat actor and has a differing degree of severity depending on the actor's capability (knowledge and experience, access to weapons, tools and means of assistance), intent, previous and presumed future choice of target (targeting).

Planning of a building and civil engineering works involves two aspects related to protection – protective security and safety (the latter including for example protection against fire, flood, earthquake, and technical installations failure in the building and civil engineering works). The two aspects can, under some circumstances, generate contradictory requirements, and resolving them in a satisfactory manner is a very important task at the planning and design stage. A typical example of such contradictory requirements is the necessity of safeguarding effective evacuation of persons from a building in an emergency situation versus the necessity of preventing unauthorized persons from entering the building. Universal design, i.e. accessibility and egressibility[1)], is also an important aspect that needs a high degree of attention.

1) Ability to leave the building or any other delimited area.

Buildings and civil engineering works — Security — Planning of security measures in the built environment

1 Scope

This document provides requirements and recommendations for effective planning and design of security measures in the built environment.

The purpose of the document is to achieve optimal protection of assets against all kinds of malicious acts, while ensuring functional, financial, and aesthetic aspects.

The document describes which methods and routines need to be implemented in various stages of a building or civil engineering works project, as well as the competencies needed to achieve a good result.

This document is applicable to new builds, refurbishments and development projects by government and private entities, for various environments, buildings and infrastructure.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 6707-1, *Buildings and civil engineering works — Vocabulary — Part 1: General terms*

ISO 19650-5, *Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling — Part 5: Security-minded approach to information management*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 6707-1 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
security
state of relative freedom from *threat* (3.18) or harm caused by deliberate, unwanted, hostile or malicious acts

[SOURCE: ISO 19650-5:2020, 3.7]

3.2
protective security
use of measures when managing *risk* (3.20) linked to undesirable intentional actions

3.3
preventive security
planning, preparation, implementation and overseeing of *protective security* (3.2) measures which seek to eliminate or reduce *risk* (3.20) resulting from a *threat* (3.18)

3.4
actor
organization or individual that fulfils a role

3.5
project stage
delimited stage within a project

Note 1 to entry: A project stage can in turn be divided into sub-processes. The division is often justified on the basis of identifying deliverables, decisions, and changes of *actors* (3.4). It can be adapted to the individual organization or situation.

3.6
strategic definition
project stage (3.5) during which the justification, overarching aim, and framework of the project are identified

3.7
preparation and brief
project stage (3.5) during which it is ascertained whether the project is feasible, and determined which conceptual solution is most appropriate

3.8
concept design
project stage (3.5) during which principles are developed for a technical solution with realistic strategies and plans for the project, so that a final decision on implementation can be made on a correct basis

3.9
developed design
project stage (3.5) that includes coordinated and updated proposals for structural design, building services systems, outline specifications, cost information and project strategies in accordance with the design programme

3.10
technical design
project stage (3.5) that occurs after the *developed design* (3.9) has been completed and in which the residual technical work of the core design team is completed

3.11
construction
project stage (3.5) during which deliverables are completed in accordance with plans and intentions

3.12
testing and handover
project stage (3.5) during which a fault-free technical delivery is handed over and it is ensured that all systems are correctly adjusted to their intended use

3.13
user
organization or person which uses or is intended to use, a building or other construction works

Note 1 to entry: A user can also be the owner of the building or construction works.

[SOURCE: ISO/TR 15686-11:2014, 3.1.131, modified — "animal or object" has been deleted; Note 1 to entry has been deleted and replaced with a new Note 1 to entry; cross-references to terminological entries in ISO 6707-1 have been removed.]

3.14
in use
project stage (3.5) during which technically sound and economic operation is ensured that satisfies the user's requirements to the project and that provides the intended effect

3.15
decommissioning
project stage (3.5) during which a viable and prudent conclusion to ownership or period of use is ensured

3.16
asset
item, thing or entity that has potential or actual value to an organization

Note 1 to entry: Value can be tangible or intangible, financial, or non-financial, and includes consideration of *risks* (3.20) and liabilities. It can be positive or negative at different stages of the asset life.

Note 2 to entry: Physical assets usually refer to equipment, inventory and properties owned by the organization. Physical assets are the opposite of intangible assets, which are non-physical assets such as leases, brands, digital assets, use rights, licences, intellectual property rights, reputation, or agreements.

Note 3 to entry: A grouping of assets referred to as an asset system could also be considered as an asset.

Note 4 to entry: Life, health and welfare of humans and other living beings can also be an asset.

Note 5 to entry: In the context of this document, organization can be understood as both owner and user of the physical asset in question.

[SOURCE: ISO 55000:2014, 3.2.1, modified — Notes 4 and 5 to entry have been added.]

3.17
vulnerability
lack of resilience against an undesirable intentional action or inability to recover a new stable condition of an *asset* (3.16)

3.18
threat
potential, deliberate action that can cause harm to an *asset* (3.16)

Note 1 to entry: A threat is always related to a threat *actor* (3.4), which can be an individual or an organization.

3.19
design-basis threat
threat (3.18) used as a basis for preparing security measures

3.20
risk
effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and *threats* (3.18).

Note 2 to entry: Objectives can have different aspects and categories, and can be applied at different levels.

Note 3 to entry: Risk is usually expressed in terms of risk sources, potential events, their consequences, and their likelihood.

Note 4 to entry: In the context of *protective security* (3.2) against threats, risk is usually expressed in terms of threat, impact, and *vulnerability* (3.17).

Note 5 to entry: In the context of this document, risk is used as a negative deviation.

[SOURCE: ISO 31000:2018, 3.1, modified — Notes 4 and 5 to entry have been added.]

3.21
residual risk
risk (3.20) remaining after risk treatment

Note 1 to entry: Residual risk can contain unidentified risk.

Note 2 to entry: Residual risk can also be known as “retained risk”.

Note 3 to entry: “Risk treatment” in this document means carrying out mitigating measures to reduce the risk.

[SOURCE: ISO Guide 73:2009, 3.8.1.6, modified — Note 3 to entry has been added.]

3.22
risk assessment
overall process of *risk* (3.20) identification, *risk analysis* (3.23) and risk evaluation

[SOURCE: ISO Guide 73:2009, 3.4.1]

3.23
risk analysis
process to comprehend the nature of *risk* (3.20) and to determine the level of risk

Note 1 to entry: Risk analysis provides the basis for risk evaluation and decisions about risk treatment.

Note 2 to entry: Risk analysis includes risk estimation.

[SOURCE: ISO Guide 73:2009, 3.6.1]

3.24
stakeholder
person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

Note 1 to entry: A *decision maker* (3.25) can be a stakeholder.

[SOURCE: ISO Guide 73:2009, 3.2.1.1]

3.25
decision maker
top management or a person designated by the top management, and given delegated authority to make decisions

3.26
principal
person or organization that has initiated the project

Note 1 to entry: Principal can correspond to "developer" or "client".

3.27
project manager
person with the responsibility for planning, executing, and closing off a project

3.28
supplier
person or organization supplying materials or products

Note 1 to entry: In this document, supplier can also mean person or organization supplying services.

[SOURCE: ISO 6707-2:2017, 3.8.30, modified— Note 1 to entry has been added.]

3.29
security deliverable
security-specific written report, memorandum, drawing, digital information model, product solution or other documentable work based on specialist professional input

Note 1 to entry: The security deliverable is normally a sub-element of or input to the project to be executed.