DRAFT INTERNATIONAL STANDARD

ISO/DIS 23234

ISO/TC **59**	Secretariat: **SN**
Voting begins on: **2020-04-13**	Voting terminates on: **2020-07-06**

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

ICS: 93.010; 91.040.01

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/96b467ad-f7d6-48d8-982a-4dc205d79d93/iso-dis-23234

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

Reference number
ISO/DIS 23234:2020(E)

© ISO 2020

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/96b467ad-f7d6-48d8-982a-4dc205d79d93/iso-dis-23234

COPYRIGHT PROTECTED DOCUMENT

© ISO 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO 2020 – All rights reserved

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/DIS 23234:2020
https://standards.iteh.ai/catalog/standards/sist/96b467ad-7fd1-48d8-982a-4d205d79d93/iso-dis-23234

© ISO 2020 – All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/96b467ad-f7d6-48d8-982a-4dc205d79d93/iso-dis-23234

© ISO 2020 – All rights reserved

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/96b467ad-f7d6-48d8-982a-ad2053b9d93/iso-dis-23234

© ISO 2020 – All rights reserved

Introduction

General

The objective of the standard is to provide recommendations on how enterprises should effectively plan security measures in order to protect their built environment (e.g. buildings, plants, infrastructure and property) against undesirable intentional actions. The standard can be used by all enterprises that seek physical security to be part of their protection against undesirable intentional actions.

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

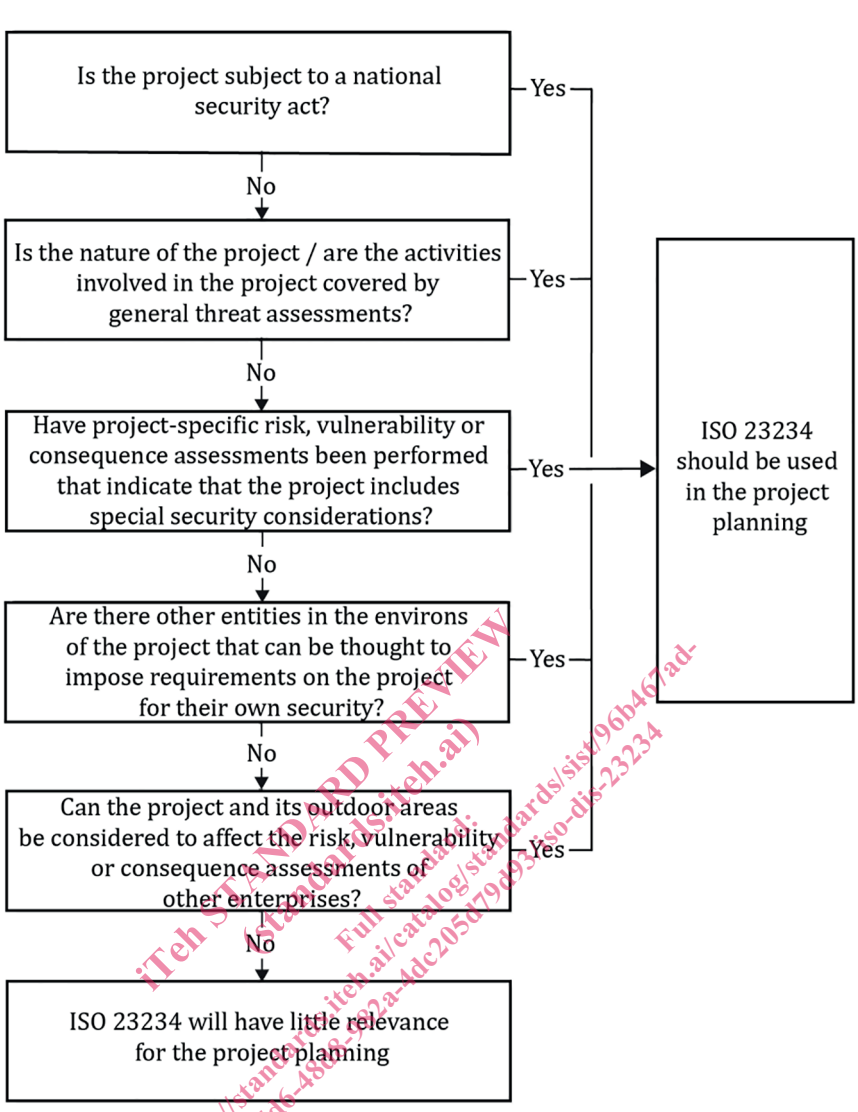
This standard describes an approach to planning security measures in the built environment based on generic stages and corresponding security deliverables in each stage. The standard also defines a number of roles that should be assigned in the project organization to ensure that the security input to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

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

Figure 1 shows a checklist for when the standard becomes applicable.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/96b467ad-f7d6-48d8-982a-4dc205d79d93/iso-dis-23234

© ISO 2020 – All rights reserved



iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/96b467ad-f7d6-4808-922a-4dc205d79d93/iso-dis-23234

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

National security regulations

In addition to the requirements ensuing from the enterprise's own risk acceptance, enterprises that are subject to national security regulations (where they exist) could be obliged by law to protect critical assets and functions. For enterprises not subject to such regulations, it will be natural to base their approach on the insurance companies' requirements for their basic security. This standard is general in nature and for general use, both within and outside of the scope of application of national security regulations.

Safety and security

The standard is targeted primarily at the domain referred to as protective security. In this standard the common words "safety" and "security" are used to distinguish between methods of combating undesirable unintentional incidents or accidents (safety) and combating undesirable intentional actions (protective security). In this sense, protective security is an action performed to provide protection against an actor with a deliberate undesirable intention towards an asset.

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 this specific threat". The threat will derive from a threat actor and will have a differing degree of severity depending on the

© ISO 2020 – All rights reserved

actor's existence, capability (knowledge and experience, access to weapons, tools and means of assistance), intent, previous and presumed future choice of target (targeting).

The security aspects shall be coordinated at all stages of the building process with safety aspects (the latter including for example protection against fire, flood, earthquake, and technical installations failure in the building). The two aspects can, under some circumstances, generate contradictory requirements, which must be resolved in a satisfactory manner at the planning and design stage. A typical example of such contradictory requirements is the necessity of safeguarding effective evacuation of persons from the building in an emergency situation versus the necessity of preventing unauthorized persons from entering the building. Universal design, i.e. accessibility and egressibility[1)], must also be taken into consideration.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/96b467ad-f7d6-48d8-982a-4dc205d79d93/iso-dis-23234

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

© ISO 2020 – All rights reserved

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 should 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/96b467ad-f7d6-48d8-922a-46205d7d93eb/iso-dis-23234

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/DIS 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 following terms and definitions given in ISO 6707-1, ISO/DIS 19650-5 and the following apply.

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

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

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

3.1
security
state of relative freedom from *threat* (3.20) or harm caused by deliberate, unwanted, hostile or malicious acts

[SOURCE: ISO/DIS 19650-5, 3.7]

3.2
protective security
use of measures when handling *risk* (3.22) linked to *undesirable intentional actions* (3.19)

3.3
preventive security
planning, preparation, implementation and overseeing of protective security measures which seek to eliminate or reduce *risk* (3.22) resulting from an activity that poses a *threat* (3.20)

© ISO 2020 – All rights reserved

3.4
entity
individual, organization, state, grouping, enterprise, physical object or any other unit that fits the context

Note 1 to entry: In this standard, an entity will primarily be a physical object, such as a building, plant or property or a part thereof. Examples of this are an enterprise, a building, a room for storing encryption material or a security component such as an access control unit.

3.5
actor
entity (3.4) that fulfils a role

Note 1 to entry: An actor can be an organization or an individual.

3.6
project stage
delimited stage within a project

Note 1 to entry: A project stage may in turn be sub-divided into sub-processes. The division is often justified on the basis of identifying deliverables, decisions and changes of *actors* (3.5). It is to be adapted to the individual enterprise or situation.

3.7
strategic definition
project stage (3.6) in which the justification, overarching aim and framework of the building project are identified

3.8
preparation and brief
project stage (3.6) in which it is ascertained whether the building project is feasible, and it is determined which conceptual solution is most appropriate

3.9
concept design
project stage (3.6) in which principles are developed for a technical solution and realistic strategies and plans for the building project, so that a final decision on implementation can be made on a correct basis

3.10
developed design
project stage (3.6) including co-ordinated and updated proposals for structural design, building services systems, outline specifications, cost information and project strategies in accordance with the design programme

3.11
technical design
project stage (3.6) which occurs after the developed design has been completed and in which the residual technical work of the core design team is completed

3.12
construction
project stage (3.6) in which deliveries are performed in accordance with plans and intentions

3.13
testing and handover
project stage (3.6) in which a fault-free *entity* (3.4) is handed over and it is ensured that all systems are correctly adjusted to their intended use

3.14
in use
project stage (3.6) in which technically sound and economic operation is ensured that satisfies the user's needs from the project and provides the intended effect

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/76b467ad-f7d6-4dd8-982a-4dc205d7d93/iso-dis-23234

© ISO 2020 – All rights reserved

3.15
disposal
project stage (3.6) for ensuring a viable and prudent conclusion to ownership or the building's period of use

3.16
asset
item, thing or *entity* (3.4) 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* (3.22) 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 standard, organization can be understood as both owner and user of the built environment 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* (3.19) or inability to recover a new stable condition of an *asset* (3.16) subject to an undesirable impact

3.18
undesirable incident
incident that can have an undesirable impact on an *asset* (3.16)

Note 1 to entry: Undesirable impact on an *asset* (3.16) can for example be destruction, appropriation or disturbance.

Note 2 to entry: Undesirable unintentional incidents can be caused by natural elements and technical or human failure.

3.19
undesirable intentional action
undesirable incident (3.18) that is caused by an *actor* (3.5) (perpetrator) acting with a purpose

Note 1 to entry: The *actor's* (3.5) purpose can be malicious or hostile.

3.20
threat
potential, deliberate action that can cause harm for an *asset* (3.16)

Note 1 to entry: A threat is always related to a threat perpetrator, which can be an individual or an organization.

3.21
design-basis threat
threat (3.20) used as a basis for preparing security measures

3.22
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* (3.20).

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/96b4f7ad-f7f6-48d8-832a-4bc205d79d93/iso-dis-23234

© ISO 2020 – All rights reserved