INTERNATIONAL STANDARD

ISO 23234

First edition
2021-02

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 23234:2021(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.

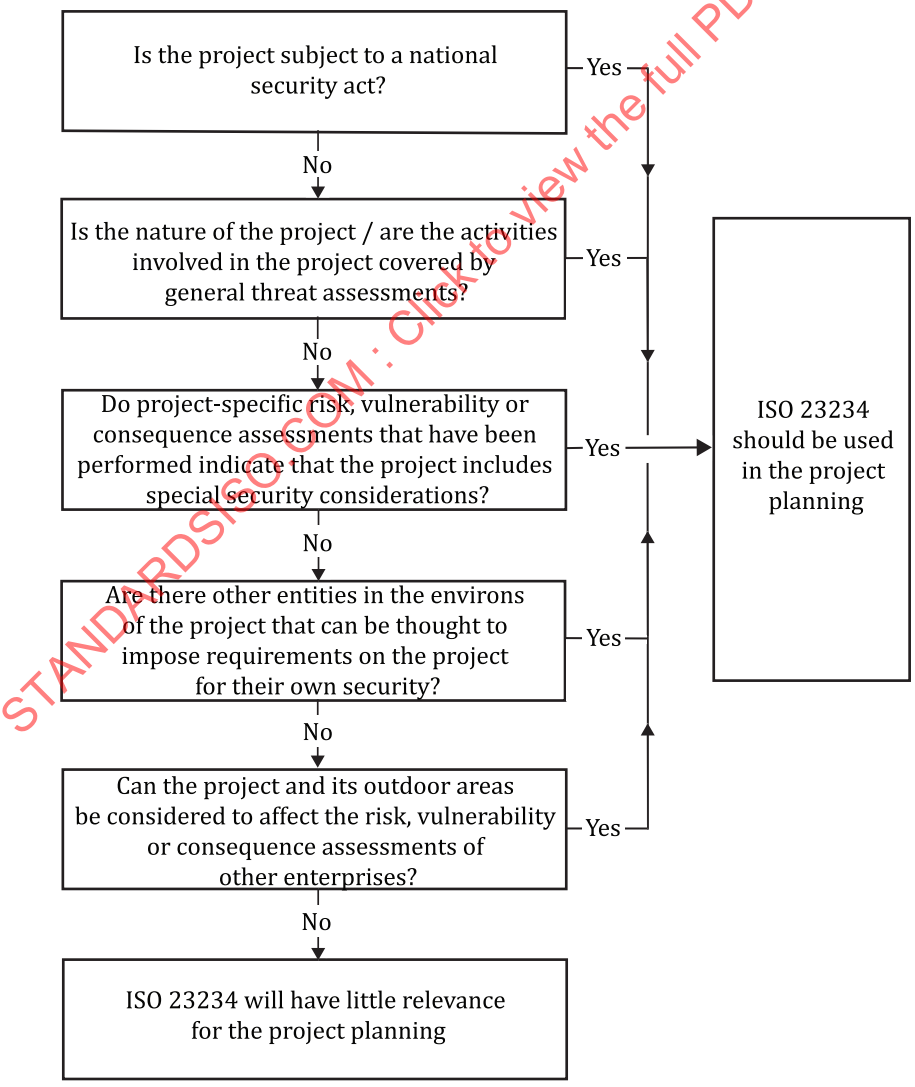

Figure 1 — Checklist as guidance for possible use of ISO 23234 in built environment projects

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 for 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.

3.30
external policy maker
external *actor* (3.4) that sets guidelines for the project and whom the project has little opportunity to influence

Note 1 to entry: External policy makers can include the police, planning and building authorities, heritage authorities, other public authorities, standards-setting bodies, etc.

3.31
security planner
adviser with knowledge and experience in managing the planning of the security works in construction projects with special security requirements

3.32
security risk adviser
adviser with knowledge and experience in undertaking *risk assessments* (3.22)

3.33
technical security adviser
adviser within a technical subject with special knowledge and experience in *security* (3.1) during the operational phase of the process

Note 1 to entry: This can include engineers with specialist knowledge and experience in the *vulnerability* (3.17) and security of structures, electro-technical installations, or other systems. This can also include architects or landscape architects with specialist knowledge and experience in security.

3.34
operational security adviser
adviser within the domain of human and organizational security measures during the operational phase of the project

Note 1 to entry: This role is often filled by the user's own security organization.

4 Planning of security measures for the built environment

4.1 General

Where there is an identified need for protective security in relation to an asset in the built environment, protective security measures shall be considered and, where implemented, managed in all project stages.

This document sets out a suggested model for project stages (see Table 1) that can be applied whether a project relates to a new or existing asset. Some projects might follow alternative project models for the execution of work. Depending on the nature of the project, the complete model can be followed, or parts can be adapted and applied.

The actors in a construction process have defined tasks and roles in the different stages and sub-processes. The principal is responsible for defining the construction programme and detailed requirements, while the project manager and project planning manager are responsible for ensuring that the decision support documentation for security is prepared in line with the accepted recommendations of the project security adviser and to the right quality. The project planners shall jointly develop the project from a list of needs and functions that result in suggestions for detailed interdisciplinary solutions. The project executors shall deliver and implement the selected solutions, and document that their execution complies with the defined requirements.

All actors involved in the project security works shall familiarise themselves with the requirements and instructions defined by the principal in the project and understand how the security requirements also affect the individual's specialism and choice of solutions. This document describes the tasks, functions, and responsibilities of the protective security roles during the individual stages. This should be viewed in relation to other security deliverables in the construction project. Requirements for protective security measures shall be developed in the project in the same way as other functions

and requirements. Security requirements should be defined through processes for security risk management in the principal's organization before the project is established.

4.2 Security planning as part of risk management

In a construction project where protective security measures are to be implemented in accordance with this document, there can often be a number of activities in parallel with, or in advance of, what is defined as the construction project itself. During the planning processes, public stakeholders should be asked whether their needs are sufficiently taken into account.

The principal shall decide which security measures to implement. The basis for such recognition often emerges from the organization performing security risk assessments as an on-going activity in the organization's security risk management.

The organization is expected to have ongoing processes for mapping, analysing, and assessing its threat profile in relation to assets and known threats. Changes in the asset inventory or the threat picture can result in the need to alter security measures. The same can be true after incidents that have affected the organization.

Which security deliverables are included at each stage within a specific construction project depends on the nature of the project and how it is being organized. Sometimes, a security risk analysis has already been conducted by the principal before the construction project begins. The project organization can then use the security risk analysis as supporting documentation for its work.

The principal can choose to include the introductory security deliverables in the strategic definition project stage, as part of its ongoing operations, as a concept for the construction project, or as the first stage of the construction project. A construction project organised in accordance with this document shall always use design-basis threats and security risk analyses in the project planning and execution of the security works.

4.3 Size of projects

Organizations with a need for security measures against undesirable intentional actions shall perform mapping, assessments, and analyses as a basis for their choice of final security measures. The organization and scope of the work should be modified according to the type and size of the project. For smaller projects, it can be appropriate to use this document for parts of the process only, and the security deliverables can have a lesser scope. This gives the organization the opportunity to adapt the usage of this document to its own needs.

4.4 Division of the building process into stages

4.4.1 General

The deliverables in the stage descriptions show which information and documentation is necessary to complete the project tasks during that individual stage.

Table 1 shows where the individual security deliverables belong in different stages of the construction project.

Table 1 — Project stages and security deliverables

Step 1	Step 2	Step 3	Step 4	Step 5	Step 6	Step 7	Step 8
Strategic definition	**Preparation and brief**	**Concept design**	**Developed and technical design**	**Construction**	**Testing and handover**	**In use**	**Decommissioning**
Impact assessment	Input to the dependency map	Reassess security objectives	Input to tender drawings	Participation in implementation control	Participation in handover	Contributions to trial use	Overview of sensitive installations
Security objectives	Security risk analysis (preparation and brief)	Security risk analysis (concept)	Input to delivery and job descriptions	Participation in functional tests and commissio-ning	Completeness check	Security training	Security risk assessment (decommissioning)
Requirements for security planning	External requirements report	Reassess security measures	Contributions to tender evaluation	Input to the operations and maintenance manuals	Quality and functionality check	Security verification	
Threat assessment, scenario selection and design-basis threat	Security strategy	Description of security measures		Input to operational requirements			
Security risk analysis (strategic)	Input to zoning plan	Integration of security measures		Requirements to main-tenance and alterations of security measures			
	Input to functional programme	Selection of security measures		Assessment of final design			
	Identifying and assessing security measures	Input to operational requirements		Assessment of as built design			
	Quantity survey for preparation and brief	Quantity survey for concept					
	Contributions to preliminary design report						

4.4.2 Strategic definition

Within the strategic definition stage, the purpose and framework of the construction project, to meet the user needs and requirements (where known), are identified and a business plan prepared.

The degree of protection required to mitigate the risks posed by identified potential threats to the completed building or infrastructure, the services delivered from or by it, or specific sensitive assets contained within or on it, shall also be defined.

The principal then assesses if the construction project is commercially viable and whether to continue the planning or not.

4.4.3 Preparation and brief

During the preparation and brief stage, conceptual solutions are developed to establish whether the construction project as set out in the strategic definition stage is feasible. By the end of this stage, the most appropriate conceptual solution is determined based on the organization's general business plan, provisional business plan for the construction project (justification and strategic objective) and a requirements analysis linked to the construction project.

Opportunities and preconditions for the project are investigated and the objectives, framework, and success criteria for the project are specified. The stage also involves the definition of the functional and spatial requirements.

At the end of this stage a conclusion is reached as to whether to proceed with the project or not.

4.4.4 Concept design

The concept design develops the principles for a technical solution and the strategies and plans for the construction project so that a final decision on implementation can be made.

During this stage, the following shall be produced:

— a verified specification of the user's needs and requirements;

— a study of functions and solutions;

— the expected impact assessment of the protective measures; and

— a confirmed business plan for the project.

These shall allow a final project scope, a specific execution plan and a cost estimate to be produced and enable the organization to reach a final decision on the financing and execution the project.

4.4.5 Developed and technical design

During the developed and technical design stage, detailed and quality-assured design documents are produced, as well as the final project scope and execution strategy with associated costs (including estimates of uncertainty margins), schedule, and quality requirements. The suppliers shall also submit detailed information on systems and products.

In this stage, the principal shall decide where any specialist personnel, materials and systems are required during the project and for the completed building or infrastructure, based on the information set out in the user requirements.

The purpose of documentation produced in this stage is to ensure that the construction project can be completed to the right quality at the right time.

4.4.6 Construction

During the construction stage, work should be undertaken according to the design documentation and other associated requirements.

In this stage, the principal shall ensure that qualified persons take necessary decisions in compliance with the business plan and user's needs.

A plan should be developed for testing of relevant components and systems and a quality assurance review of the completed works shall be undertaken. By the end of the construction stage, "as built", operation and maintenance documentation shall be submitted to the principal.

4.4.7 Testing and handover

By the conclusion of the testing and handover stage, the completed works should be fault-free and all systems should be correctly adjusted for their intended use before the construction works is handed over to the principal, together with any testing and certification documentation.

During the trial use period, operating personnel and users should also be trained in the use of any specialist systems.

At the end of the trial use period, the principal assesses whether the completed project complies with the business plan and accepts (or rejects) the results of tests and reports from the trial.

As a result of the work during this stage, finished construction works, quality-assured with functional tests, trial use and inspections, emerges. The user monitors the functions of the product and assesses the performance.

4.4.8 In use

During the in-use stage, the construction works should be operated according to the needs of the user; and its performance, as well as the performance of specific systems, should be monitored and recorded.

4.4.9 Decommissioning

Decommissioning occurs when the current use or ownership of a construction works comes to an end. During this stage, it can be necessary for current assets to be removed, especially where the owner or user considers that the assets are of a sensitive nature. The assets can also be replaced by other assets belonging to new users.

During this stage, the principal keeps final accounts and performs analyses, while the user's participation ceases.

If the construction works, or in the case of demolition, the site, is sold, all relevant documentation shall be transferred to a new owner.

4.5 Organization and principal

The organization becomes a principal (buyer, client) when it decides to carry out a construction project. The principal can sometimes be the intended user of the final outcome of the project.

The principal can choose to:

— sell the finished construction works to a buyer unknown at the planning stage;

— sell the finished construction works to a buyer known at the planning stage;

— continue to own the construction works after completion and rent it to a user unknown before completing the works;

— continue to own the construction works and rent it to a user known before completing the works; or

— continue to own the construction works and use it for own purposes;

and the selected alternative can determine the choice of the security measures to be implemented before take-over of the final outcome of the project.

If the building or infrastructure is sold to a buyer who remains unidentified until the building or infrastructure is finished, the security measures implemented might not meet the requirements of the

end user. Under such circumstances, future users should conduct their own analysis and implement security measures based on their needs.

When the principal intends to rent the building or infrastructure to a pre-identified user, the planning of security measures is likely to be based on the requirements contained in the contract between the principal and the end user.

4.6 Special advisers in security projects

4.6.1 General

In addition to the general roles pertaining to construction projects, irrespective of their arrangement, projects with special security needs also require specialist knowledge and experience. This document therefore defines five specialised roles that in turn can have sub-specialisms. The five specialised roles are:

— security planner;

— security risk adviser;

— technical security adviser, which includes roles such as specialised architect and landscape architect, structural adviser, and systems adviser;

— operational security adviser; and

— project security adviser.

NOTE For these roles, there are currently few dedicated training programmes or certification schemes. In most projects, it is therefore up to the principal, project manager or project planning manager to define the need for such roles, with detailed specification of the associated knowledge and experience, and to assess whether such skills need to be possessed by an individual adviser or a group of advisers.

4.6.2 Security planner

A security planner is an adviser with knowledge and experience in managing the planning of the security works in construction projects with special security needs.

The security planner has experience of project management and a good understanding of the disciplines that are most important for security work. A security risk adviser, technical security adviser and operational security adviser can act as a security planner if they possess those qualifications.

For projects where security constitutes a significant part of the deliverables, the project manager or project planning manager can act as the security planner if they have sufficient insight into the necessary deliverables and the knowledge and experience required for the security deliverables.

4.6.3 Security risk adviser

A security risk adviser is an adviser with sufficient knowledge and experience in the entire assessment process of threat, vulnerability and risk in relation to the functional design and location of the construction works. This adviser is able to advise on security objectives, prepare scenarios, visualise the risk picture and evaluate strategies.

The security risk adviser shall have sufficient knowledge to:

— assess the practical performance of qualitative assessments;

— analyze the validity and reliability of the information supporting the assessments;

— estimate impact assessments, threat assessments, security reviews and audits;

— estimate the need for security measures of the client;

— estimate the positive and negative effects that can result from a security measure;

— understand how combinations of measures can impact each other; and

— understand specialist domains such as manned guarding, structural barriers, surveillance, etc.

4.6.4 Technical security adviser

4.6.4.1 General

The role of technical security adviser can be filled by one or more specialists with skills in advising on vulnerability, technical security measures or the design of the construction works. Sometimes, this role has also been described as "consulting security engineer". This overarching term can cover a range of specialist roles, such as architects, landscape architects, structural advisers, systems advisers, and other technical security advisers. For projects where protective security constitutes a significant part of the deliverable, the technical security advisers can act as the security planners if they have sufficient relevant knowledge and experience in the security vulnerabilities and possible security measures.

4.6.4.2 Architect

This role presupposes an architect with specialist knowledge and experience in protecting the built environment against undesirable intentional actions.

The task of the person (or team) is to adapt architectural solutions to the requirements of protective security. An architect acting as a technical security adviser shall understand how architectural solutions influence the resilience against hostile actions, and how to adapt the initial architectural solutions to reduce the vulnerability of the building or civil engineering works.

4.6.4.3 Landscape architect

This role presupposes a landscape architect with specialist knowledge and experience in protective security, for example vehicle access conditions, the design of permanent hostile vehicle mitigation barriers with controlled access, screening of vehicular traffic, illumination, etc.

4.6.4.4 Structural adviser

A structural adviser is an adviser with knowledge and experience in performing vulnerability assessments of structures in the built environment and experience in selecting and implementing measures to protect the structure of the building, plant, or property.

The structural adviser has, for example, knowledge and experience in materials technology, construction technology, technical building standards and load-bearing properties. This adviser should also have knowledge of the dynamic response of structures to large impulse loads, e.g. the impact of full or partial collapse of the structure of a building caused by explosives, as well as knowledge of the environmental risks that can impact the structure of a building, such as earthquakes.

The structural adviser should have engineering expertise in protection against armed assaults, explosives, blast effects, and forced entry. The structural adviser should also have expertise in measures such as hostile vehicle mitigation, pedestrian barriers, weapon detection, etc., and special knowledge of protective security through the use of glazing, building materials (concrete, masonry, metal, wood, plastic, composites), infrastructure/installations, earth/rock, etc.

4.6.4.5 Systems adviser

The systems adviser is an adviser who has knowledge and experience in performing vulnerability assessments of the technical installations in a construction works, documented insight into technical system relations and dependencies, and experience in selecting and implementing technical security measures.

Depending on the project, the systems adviser has knowledge and experience with the relevant electro-technical standards, the benefits and disadvantages associated with different types of electronic security systems, location-specific considerations, effects of individual or concurrent faults in the systems and system integration.

For projects where protective security constitutes a significant part of the deliverables, the consulting electro-technical engineer can act as the security planner if they have sufficient relevant knowledge and experience in the security vulnerabilities and possible mitigation measures that are relevant for the project.

Systems advisers include engineers with specialist knowledge and experience with electronic security systems, including closed circuit television (CCTV), intrusion detectors, perimeter sensors, automatic access control systems, security-related lighting, control room systems, computer networks, etc.

4.6.4.6 Other technical security advisers

Technical security advisers can also include advisers with specialist knowledge and experience in the design of security measures linked to ventilation, detection of chemical, biological, radiological, and nuclear weapons, detection of explosives and other technical protective security domains.

A technical security adviser can also have special knowledge and experience in vehicle dynamics, topography, materials, and equipment testing.

4.6.5 Operational security adviser

An operational security adviser has knowledge and experience of human and organizational security measures. An operational security adviser shall provide advice on operational security aspects such as the use of rapid reaction forces, surveillance, etc. An operational security adviser shall contribute to the vulnerability assessment of the functional design and siting of the construction works and property.

While the human and organizational security measures should be coupled with the technological measures as part of the project's deliverables, they often do not constitute part of the construction project. An operational security adviser gives advice about resource consumption and management linked to detection, verification, and reaction. Among other things, this entails advice on the planning, sizing and use of manned guarding forces, the organization, verification, and assessment of received sensor data and the development of decision support systems and operational action plans.

The knowledge and experience of operational security advisers should be based on a combination of formal training and experience within operational domains. An operational security adviser shall possess understanding of how human and organizational security measures function in the finished building, plant, or property, and how these measures function in combination with the technical security measures.

4.6.6 Project information security adviser

The responsibility for ensuring that project information is properly protected should be assigned to an appropriate individual(s). Appropriate document and information-handling routines, protection and special authorisation schemes for personnel working on the project (security clearance / authorisation for certain projects), etc., should be put in place. The project's information security management shall be organized according to ISO 19650-5. The project information security adviser should have good knowledge of information security challenges ensuing from the use of building information models (BIM).

5 Security deliverables in stages

5.1 Strategic definition

5.1.1 Asset inventory

An asset inventory is part of a security risk assessment. This includes identification of the most important assets, such as personnel, physical assets, information and functions.

The principal (or the future user, if not the same) shall have a complete inventory of the assets it owns or has available and understand what the assets represent. In addition, all relationships to other organizations shall be mapped and assessed.

An asset inventory is part of a security risk assessment and evaluates the role of different assets in the organization's function, and the consequences of their disruption or loss. Each asset is assessed separately and described as to what it is and how it is used.

The next steps are threat assessment and impact assessment.

The threat assessment and impact assessment are performed by the security risk adviser and the principal, supported by a security planner if needed.

NOTE It can be relevant to look at the potential for harm through the compromise or improper disclosure of information (breach of confidentiality), the tampering with or improper modification of information (damage to integrity) and the destruction of information or functions (damage to availability).

5.1.2 Protective security objectives

Objectives shall be defined for what is a desirable or acceptable condition for the asset during or after an undesirable incident. The security objectives shall be re-evaluated later on in the construction project. These objectives define the purpose or expected outcome attributable to the security measures. The setting of objectives is based on the impact assessment and performed by the principal in consultation with the project manager, potentially with support from the security planner or security risk adviser.

The protective security objectives can be described by one or more of the following:

— definition of which threats the preventive security measure shall, as a minimum, be able to withstand (basic security) and what the consequence-reducing measures (emergency response measures) shall be able to withstand;

— definition of the longest acceptable time elapsed from the moment an undesirable incident occurs until a new, acceptable state has been achieved;

— description of the final state of the organization, i.e. the state desired to maintain or recreate once the attack has been concluded.

EXAMPLE The final state can include an assumption that persons can escape safely, that no serious personal injury would occur, that activities can be resumed, or similar. The protective security objectives can express the time it would take before an organization can resume ordinary delivery of its products or services.

Security objectives are important notably in order to make the right trade-offs and choices in the threat assessment, choice of scenarios, the vulnerability assessment, the risk assessment, and selection of strategies and measures.

The protective security objectives shall always refer to defined assets and how they shall be protected. The definition of objectives for the security measures shall be done in order to assess the vulnerability to different actions and/or incidents later in the process.

The protective security objectives should be re-evaluated in the course of the project. The objectives can be affected by changing costs or other factors that occur during the construction project.

5.1.3 Requirements for protective security planning

Requirements for protective security planning include an assessment of the organization of the protective security work, the methods to be employed and the knowledge, experience and progress that are relevant and necessary to deliver the project. Security deliverables and their responsible actors shall be identified for each stage in the project. Divisions of responsibilities and interfaces with applicable legislation shall be clarified.

Requirements for security planning shall be performed by the principal or project manager, in consultation with the project security adviser and the security planner.

The requirements for security planning are contained in an initial project plan that indicates which security deliverables are relevant at the different stages of the project, and the actors responsible for the delivery and approval of the security deliverables. The project plan also defines the detailed expertise expected of the security risk adviser, technical security adviser and operational security adviser. The document also assesses whether each of these roles can be filled by a person or whether a team with complementary expertise is needed.

The project plan also outlines the need for involvement of the principal and external policy makers and stakeholders at different stages of the security work. This includes the start-up of any planning work, exemption applications to authorities, etc. Requirements for security planning also entail assessment of the relationship to legislation, standards, and other factors to which the project shall respond.

The results of the security deliverable "requirements for security planning" should be transferred to the overall project plan.

5.1.4 Threat assessment, scenario selection and design-basis threats

During this stage, relevant threats and scenarios shall be identified and design-basis threats defined.

The work at this stage is conducted by a security risk adviser. Design-basis threats shall be reviewed and approved by the principal.

The threat assessment, scenario selection and definition of the design-basis threats are conducted by the security risk adviser through five stages:

a) identification of potential threat actors;

b) assessment of the threat actors' capability, intentions, history and targeting;

c) assessment of the actors' modus operandi;

d) outline of attack scenarios;

e) definition of design-basis threats.

Categories of threat actors can range from nation states, through terrorists and criminals to activists. The threat actors can be external or internal.

Each relevant actor shall be assessed in relation to the assets. Actors who are assessed as potentially having hostile intentions shall be entered on a list.

Furthermore, it shall be assessed how each potential threat actor can act to attack the target (modus operandi).

Based on the threat assessment, the security risk adviser prepares a list of possible scenarios. A scenario describes how relevant threat actors can deliberately damage or take over the assets. The scenario description shall be as specific and unambiguous as possible, so that it clearly indicates vulnerabilities and needs for measures. A scenario shall be developed for each unique pair of an asset and a threat actor.

A sufficient number of scenarios should be developed in order to get a clear picture of the challenges at hand. While too many scenarios can make the analysis too complex and unwieldy, too few scenarios can

constitute an inadequate basis for analysis. For certain projects, there can be just a few scenarios. For large and complex projects, a large number of scenarios should be generated.

From the threat assessment and scenarios, a list of design-basis threats should be derived.

Design-basis threats are selected based on known or expected capabilities among the potential threat actors, and not based on the means of attack that can theoretically be used against an asset (for example, an explosive charge).

Uncertainty concerning the information source for the threat assessment and uncertainty of the assessment itself shall be identified and should be clearly communicated.

The uncertainty of the assessment increases as the assessment's time horizon expands. For the long term, the assessment should not just be based on presently known threat actors and their capabilities. Entire categories of possible threat actors with their range of capabilities and modus operandi should be included in the assessment. Sometimes, it can be a known fact that it is difficult to protect against threats of a certain scope and consequently, the principal is willing to accept the risk of these threats being realised. The principal shall approve the final list of design-basis threats and this list constitutes supporting documentation for the future security work. The list of design-basis threats shall also be accompanied by a list of threats, if any, that the principal has decided to classify as irrelevant.

NOTE The International Atomic Energy Association (IAEA) refers to design-basis threats as "the attributes and characteristics of potential insider and/or external adversaries who may attempt unauthorized removal or sabotage, against which a physical protection system is designed and evaluated."[6]. The US Department of Homeland Security (DHS) defines design-basis threats as "a profile of the type, composition, and capabilities of adversaries"[7].

5.1.5 Information security for the project

During this stage, the need for protection of information in the project shall be described, as well as the information security measures. This work shall be performed in accordance with ISO 19650-5.

5.1.6 Security risk analysis (strategic)

During this stage, the security risk adviser shall assess the risk and present the risk picture.

On completion of the strategic definition project stage, the security risk adviser can assess the overall security risk based on the organization's assets, the design-basis threats against the organization, and any identified vulnerabilities. In some cases, the deliverable can require input from technical security advisers or others.

Location alternatives can be relevant for the project. The security risk analysis shall include an analysis of the risk for each location in question, based on the existing assessments of threat and impact. The vulnerabilities for each location, related to the defined scenarios and design-basis threats, should be described and ranked. It can be appropriate to prepare scenarios that take account of geographical location and/or neighbours of the different locations.

The protective security measures needed to achieve the security objectives shall be described for each of the locations. The description can be used to calculate the cost differences between the alternatives.

An analysis can also be made for the risk for external parties, for example increased security risk for neighbours resulting from the completion of the project.

5.1.7 Clarification of conditions

Before the construction project can advance to the next stage, the list of conditions, supporting documents, requirements and expectations shall be checked and verified for completeness. It shall also be ascertained that the conditions are properly understood.

This verification shall be performed by the principal or security planner.

The security deliverables described in the document are introduced in the strategic definition project stage. Assessments and decisions have likely been made by the principal before this stage. Any documentation from preceding activities can be collected and used in the project. The security planner begins by collecting any existing information and clarifying how it can be utilised in the project stages. Based on this information, the principal decides whether the project can continue.

5.2 Preparation and brief

5.2.1 Input to the dependency map

The dependency map comprises clarification of dependencies between the functions of an organization. This is done by means of a plan or a map that shows dependencies or relationships between the parts of the organization's functions with special security needs and the relationship to functions that do not have special security needs.

The clarification is performed by the security planner or operational security adviser.

An overview shall be established of necessary logistics within spaces, areas or functions with special security needs and zoning requirements.

At this stage it is necessary to consider the safety requirements that follow with the functions of the construction works and the public legislation that regulate the solutions. For example, every construction works shall allow for quick evacuation of the premises in case of fire or other dangerous situations. The security measures shall be harmonized with the safety measures in a way that excludes conflicting situations due to contradictory requirements to safety and security.

5.2.2 Security risk analysis (preparation and brief)

The security risk analysis comprises an assessment of the security risk for different proposed conceptual solutions for the construction works. A security risk analysis shall be done for each of the alternatives evaluated for the finished construction works or property. Particularly difficult security challenges should be identified so that they can be carefully monitored in subsequent deliverables.

The analysis is performed by the security risk adviser.

The security risk analysis from the strategic definition project stage can be used as an initial supporting document for this work. The report is based on the impact assessment and the design-basis threats. At this stage, the location has usually been chosen, and different concepts for construction at the same location are assessed against each other. The security risk analysis creates a vulnerability assessment for each of the concepts evaluated for the finished construction works or property.

The impact assessment, threat assessment and vulnerability analyses show the security risk involved in each concept. The risk picture shall be visualised so that the principal can assess the security risk associated with the different concepts.

5.2.3 External requirements report

During the preparation stage, the security planner shall consult external policy makers (for example, the police, planning and building authorities, cultural heritage authorities and other public authorities) for advice on security requirements and in order to map their expectations and needs in an external requirements report.

It can be necessary to establish special security zones (limited access) around the site, restrictions on traffic in neighbouring streets, emergency response measures to be prepared, etc.

5.2.4 Security strategy

The security risk adviser, technical security adviser and operational security adviser shall prepare a security strategy that defines how the organization should be protected against the defined design-

basis threats. The security strategy can include organizational needs, such as staffing and operations. It can also include any security-related instructions for the location of the construction works on the site, spacing requirements, and design. The security strategy is summarised in a document that forms part of the supporting documentation for the concept design project stage.

The security strategy shall clearly show how the organization should be protected against the defined design-basis threats. The security strategy shall show what zone partitions are intended to be established. It shall also make clear the need for organizational measures such as need of security staff and other considerations that affect the operational stage. This security deliverable includes security measures similar to what the fire protection concept offers within fire protection strategy. This includes topics such as siting of the plot, spacing requirements, entry and exit routes, building design (volume above and below ground), landscaping, etc.

5.2.5 Input to zoning

The security planner and security risk adviser shall prepare security input for zoning.

When building in un-zoned areas, or if a proposed development does not fit into the applicable zoning, a proposal for a new zoning plan shall be prepared. The security strategy's expectations shall be incorporated in the zoning plan, including access conditions, relations with neighbours, spacing distances, visibility conditions, etc. The inputs should be documented in separate documents to help protect sensitive information.

5.2.6 Input to the spatial and functional programming

The security planner and operational security adviser shall prepare functional security requirements as input to the construction project's spatial and functional programme. This shall show security requirements for each individual space, groups of spaces and for functions of the organization. It shall also be specified which spaces or areas shall have free access without security requirements.

The programme shall be updated continuously and be detailed during the two project planning stages (concept design and developed and technical design). The inputs should be documented in separate documents.

5.2.7 Identification and assessment of security measures

The security risk adviser, technical security adviser and operational security adviser shall identify and assess technical, human, and organizational requirements for security.

The security measure requirements define any absolute and recommended preconditions for security measures. They can include requirements from insurance companies and any technical requirements such as distances, the minimum strength of structures, façades, doors, windows, etc. Any preferred solutions shall be stated so that they can be used as a basis for future planning. This is important in order to achieve the security level that the asset shall maintain, and so that future work in the project incorporates both needs for solutions and associated costs.

Organizational and human security measures shall be harmonised with the technical measures in order to achieve the security objectives. For projects with an established user organization, it is appropriate to involve this body in the definition of requirements for organizational and human security measures.

5.2.8 Cost survey

The technical security adviser shall prepare a cost estimate for the identified security measures.

This constitutes the initial cost estimates. At this early stage of the project, the estimates are usually relatively general.

5.2.9 Contributions to preliminary design report

The security planner and technical security adviser shall prepare security input to the preliminary design report with alternative solutions for the implementation of the security requirements.

In the preliminary design, two or more alternative conceptual solutions are often examined, concluding in the recommendation of one concept. The preliminary design report shall show that the security requirements from the preparation stage have been implemented. It can be necessary to take out chapters concerning security as separate confidential annexes, so as not to compromise the project's information security.

5.3 Concept design

5.3.1 Reassessment of security objectives

The reassessment of the security objectives should analyse how the security measures developed in the preparation and brief reduce the risk. It should also analyse the cost of the measures and whether the security objectives are achieved by means of the proposed measures. The reassessment should clarify the residual risk remaining after the recommended measures have been implemented. The assessment shall be performed by the security risk adviser, while the principal shall either accept the residual risk or order changes in the project.

5.3.2 Security risk analysis (concept)

The security risk adviser updates the security risk analysis from the previous stage and elaborates on it for the chosen concept.

5.3.3 Reassessment of security strategy

An assessment shall be made as to whether there is a need to reassess the security strategy. The strategy for security measures shall be reviewed and an assessment made of how the strategy contributes to reducing security risk, and how the strategy is harmonized with any other requirements for the project, for example safety requirements.

The assessment shall be performed by the security risk adviser, technical security adviser and operational security adviser.

The reassessment of the security strategy is headed by the security risk adviser with input from technical security advisers (e.g. specialised architects, landscape architects, structural advisers, systems advisers) and operational security advisers. In the reassessment process the extent to which the security strategy is suitable for reducing risk is analysed (the vulnerability of the given assets to the design-basis threats).

5.3.4 Description of security measures

During the concept design stage, the design of the construction works is resolved, and a document shall be prepared that shows the placement of functions, interrelationships, relationships to the surroundings, etc. A good plan contributes to good security.

This input shall be provided by the technical security adviser.

The description of physical security measures typically includes system drawings for load-bearing structures or facades with specification of the construction principles and main dimensions. These system drawings and descriptions shall show how the structures are designed to counter the design-basis threats.

The technical security systems depend on the architectural and structural concepts described. In the systems described in the preliminary design, the preconditions associated with the specific alternative shall be described.

5.3.5 Integration of security measures

The technical security adviser shall contribute to the detailing of the main solutions and help prepare comprehensive plans, floor plans, cross-sections and elevations in which security solutions are integrated.

In the integration of security measures, further design is performed on the security measures as defined in the description of security measures. Investigations of buildability and usability are undertaken, and a conclusion shall be prepared so that the security solutions are incorporated as a natural part of the project.

5.3.6 Selection of security measures

The technical security adviser shall prepare drawings of security measures.

The justification for the choice of construction and security solutions shall be made evident through text, system drawings and other drawings. This provides input, both to the security works and the construction project in general.

As a basis for the choice of security solutions or a solution framework, the costs of permanent solutions throughout the lifetime of the construction works shall be included in the assessment and made evident in the concept design as early as possible. Security measures that require participation of staff, such as guarding, surveillance and response, require small investment costs but large operating costs, whereas technical functions such as CCTV, detectors, access control and the physical strength of structures require larger investment costs and lower operational costs.

5.3.7 Input to operational requirements

The security risk adviser, technical security adviser and operational security adviser shall prepare requirements for the operational organization and maintenance.

The operational element shall be set out with clear requirements so that these can be stipulated in operating and maintenance manuals for the final design.

5.3.8 Cost survey for concept

The technical security adviser shall update cost estimates for all security solutions.

The cost of all security solutions, both structural and systemic, shall be calculated and used as input for the concept report so that it is evident to decision makers.

For the security measures, the cost estimates made in the preparation and brief stage can be used as a baseline. As far as possible, the estimates should be based on quantities obtained from drawings and drawing annotations. The costs of unresolved or non-detailed systems shall be estimated using cost per square meter. It would be natural to do a quality check of the survey against relevant reference projects.

5.4 Developed and technical design

5.4.1 Input to tender drawings

The technical security adviser shall prepare input to tender drawings in which construction elements with security requirements are integrated and described.

In connection with the developed and technical design, tender drawings for construction, earthworks, structural work, and interior works shall be prepared, as well as drawings for technical facilities (HVAC, electrical power, and telecommunications). Security solutions shall be shown on separate drawings in order to protect sensitive information.