INTERNATIONAL STANDARD

ISO 22341

First edition
2021-01

Security and resilience — Protective security — Guidelines for crime prevention through environmental design

Sécurité et résilience — Sécurité préventive — Lignes directrices pour la prévention de la criminalité par la conception environnementale

Reference number
ISO 22341:2021(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 ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Understanding environmental context of crime and security risk **2**
5 Basics of CPTED **3**
5.1 Key considerations of CPTED 3
5.2 CPTED strategies 3
5.2.1 General 3
5.2.2 CPTED strategies for planning stage 5
5.2.3 CPTED strategies for design stage 5
5.2.4 CPTED strategies for site and social management stage 6
6 Process of CPTED implementation **7**
6.1 General 7
6.2 Oversight body, performance target statement and project team 8
6.3 CPTED process 10
6.3.1 Step 1 — Communication and consultation 10
6.3.2 Step 2 — Scope, context and criteria 10
6.3.3 Step 3 — Risk assessment 11
6.3.4 Step 4 — Risk treatment 12
6.3.5 Step 5 — Monitoring, review, recording and reporting 13
6.4 General principles for CPTED process 14
6.4.1 General 14
6.4.2 Balanced CPTED concept approach 14
6.4.3 Cost-effectiveness 14
6.4.4 Sustainability and resilience 15
6.4.5 Green environment (ecological) approach 15
6.4.6 Adaptive application 15
6.4.7 Evidence-based approach 15
Annex A (informative) **Key considerations of CPTED** **17**
Annex B (informative) **Fundamental CPTED concepts** **21**
Bibliography **23**

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 292, *Security and resilience*.

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

This document is intended to promote a common understanding of crime prevention through environmental design (CPTED) in the field of security, law enforcement and related risks, and their preventive measures, through environmental design and management.

CPTED concepts have been used since the 1970s and CPTED-style security measures can be traced to early human settlements. The term CPTED was first introduced in 1971 by C. Ray Jeffery, see Reference [5]. CPTED concepts originated from criminology and crime opportunity theories and studies. Since then, it has been included as part of many other crime prevention strategies that are utilized today. These include, but are not limited to, defensible space, broken windows theory, routine activity theory, rational choice, situational crime prevention and crime free housing.

CPTED has an increasingly sound theoretical foundation based on firm evidence of significant crime and fear reduction gained from a series of formal and rigorous evaluations in the field of environmental psychology, criminology and crime science. When well-planned and wisely implemented, CPTED improves community safety and industrial security in a cost-effective manner.

Figure 1 illustrates the framework of CPTED for crime prevention and security.

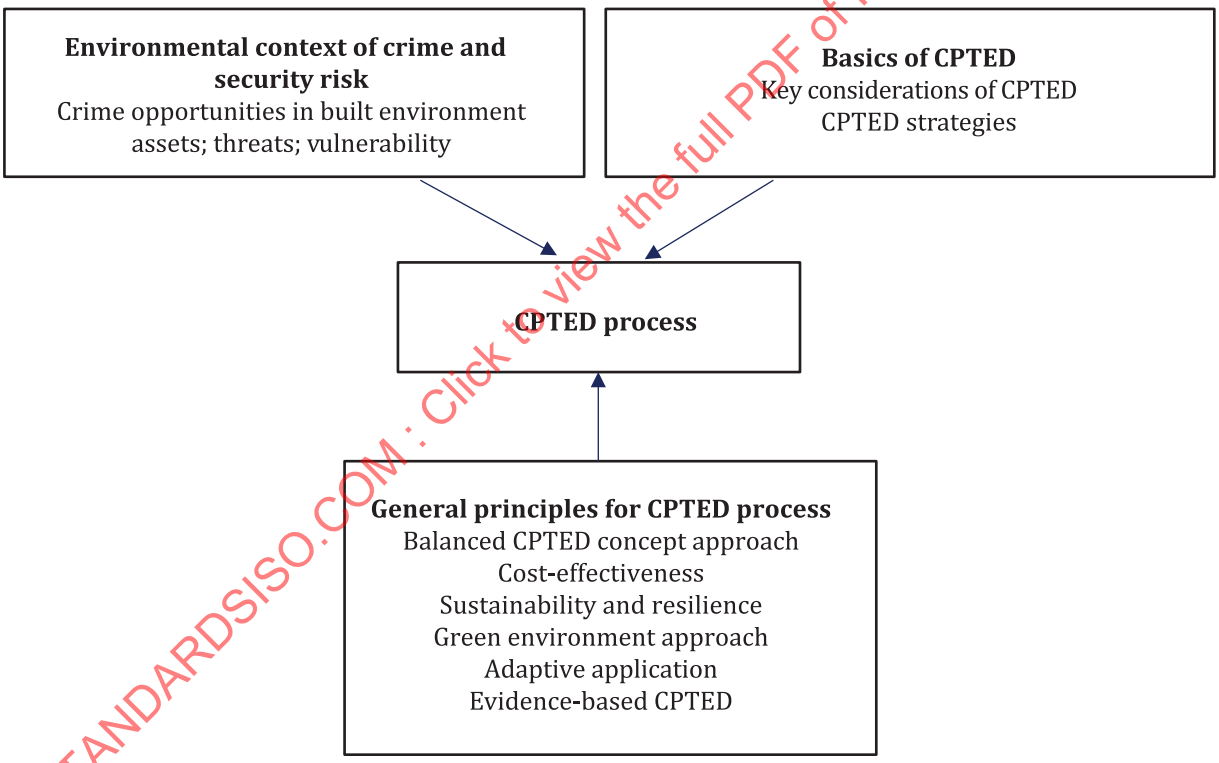

Figure 1 — Framework of CPTED for crime prevention and security

This document starts with understanding the environmental context of crime and security risk factors, causes of vulnerabilities and risk levels. This is followed by the basics of CPTED through its historical background, four key considerations of CPTED (places generating crime, types and causes of the risk, CPTED interested parties and countermeasures) and CPTED strategies. Better understanding of the risk and CPTED considerations leads to a better selection of tailored countermeasures. The process of CPTED begins with the establishment of an oversight body, performance target settings and organizing a project team, risk assessment and risk treatment, evaluation of treatment, corrective actions and feedback to the initial stage of CPTED for continual improvement. It is followed by the fundamental principles for CPTED process, such as balanced conceptual approach, cost-effectiveness, sustainability and resilience, green environment (ecological) approach, adaptive application and an evidence-based approach.

The use of CPTED should be applied universally in an equal manner and should not be applied with any prejudice (whether cultural, racial, religious or any other bias).

Security and resilience — Protective security — Guidelines for crime prevention through environmental design

1 Scope

This document provides guidelines to organizations for establishing the basic elements, strategies and processes for preventing and reducing crime and the fear of crime at a new or existing built environment. It recommends the establishment of countermeasures and actions to treat crime and security risks in an effective and efficient manner by leveraging environmental design.

Within this document, the term "security" is used in a broad manner to include all crime, safety and security-specific applications, so it is applicable to public and private organizations, regardless of type, size or nature.

While this document provides general examples of implementation strategies and best practices, it is not intended to provide an exhaustive listing of detailed design, architectural or physical security crime prevention through environmental design (CPTED) implementation strategies or restrict the potential applications to only those examples provided in this document.

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 22300, *Security and resilience — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300 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
crime prevention through environmental design
CPTED
process for analysing and assessing crime and security risks to guide development, urban design, site management and the use of the built environment in order to prevent and reduce crime and the fear of crime, and to promote and improve public health, quality of life and sustainability

Note 1 to entry: Environmental design refers to the applied arts and sciences dealing with creating the human-designed environment.

3.2
capable guardianship
willingness to supervise, detect and take action to prevent or discourage the occurrence of crime

4 Understanding environmental context of crime and security risk

There are numerous ways of defining the elements of risk.

NOTE ISO 31000 defines risk as the effect of uncertainty on objectives.

In a security context and in this document, risk is composed of three elements: assets, threats and vulnerabilities. Crime and security risks are based upon the value of the asset in relation to the threats and vulnerabilities associated with it. This approach can be viewed as an operational implementation of ISO 31000 with a specific focus on crime and security risks. Threats and vulnerabilities influence the likelihood dimension, and assets influence the consequences of a risk.

Assets can be the current state of the physical built environment and items of financial value. Assets can also be intangible with soft values.

Threats are the potential offenders or hazards and should be addressed by identifying the nature of the threat. This can be done by:

— focusing on the most likely scenarios addressed as a narrative;

— describing the subject of the scenario;

— describing the who (the offenders), where (the place of the offence) and how (what means used).

Vulnerabilities are the opportunities for negative effects and the lack of maturity related to the effectiveness of the associated countermeasures.

The crime and security risks are greater when a motivated offender and suitable target come together in time and place, without appropriate countermeasures present.

To mitigate the opportunity for a crime to occur, the conventional approach is to remove one or more of the factors expressed in the crime and security risk triangle in Figure 2. Crime events require these three factors (at a minimum) to all be present at the same time.

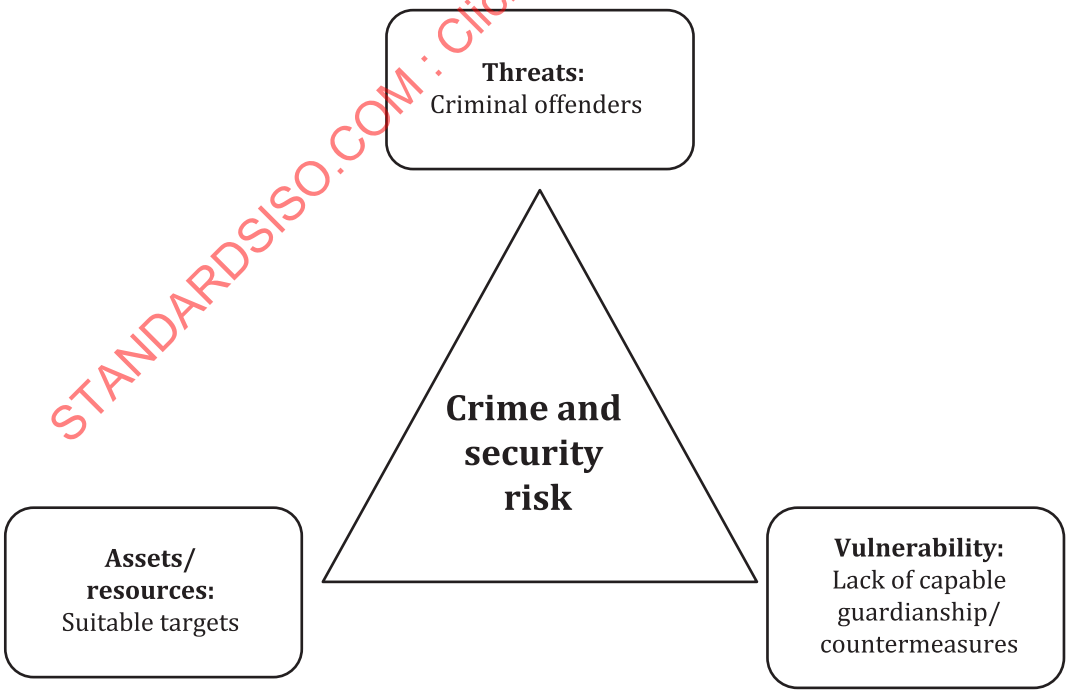

Figure 2 — Crime and security risk triangle for crime opportunities in the built environment

5 Basics of CPTED

5.1 Key considerations of CPTED

The organization should:

— base its crime prevention and security strategies on understanding crime opportunities;

— identify the following four considerations at the beginning stage of a project:

  — where: the exact location and the type of area;

  — what: the crime problems occurring in the area now or in the future;

  — who: the interested parties involved in the area;

  — how: the treatment of crime and security risks (e.g. countermeasures) in an effective and efficient manner.

NOTE Annex A provides additional information on the key considerations of CPTED.

5.2 CPTED strategies

5.2.1 General

The organization should:

— understand that there are two different CPTED concepts:

  — physical CPTED (or first generation CPTED) concept;

  — social CPTED (or second generation CPTED) concept;

— consider physical CPTED strategies as well as social CPTED strategies.

The organization should consider the six strategies for physical CPTED:

— natural surveillance;

— natural access control;

— territorial reinforcement;

— image and management/maintenance;

— activity support;

— site hardening/target hardening.

The organization should consider the four strategies for social CPTED:

— social cohesion;

— social connectivity;

— community culture;

— threshold capacity.

NOTE Annex B provides additional information about physical and social CPTED concepts and strategies.

The organization should consider three stages in order to use the physical and social CPTED strategies: planning (see 5.2.2), design (see 5.2.3), and site and social management (see 5.2.4).

Environmental planning and design stages are most relevant for proposed new areas and neighbourhoods. Management stages are more relevant in existing areas. Planning and design adaptations are relevant in existing areas to a certain degree, but the feasible adaptations are modest and small in existing areas compared to the designs for new areas.

The organization should:

— implement the CPTED strategies in order to coordinate its actions and measures;

— consider local context, cultural tradition and past experience for the actions and measures;

— select the measures in anticipation of their expected effectiveness in certain types of environments and against the prevailing types of crime.

Table 1 provides detailed information with examples on the CPTED strategies by stage.

Table 1 — CPTED strategies and examples by stage

Stage	Strategies	Examples
Planning	Avoiding blind/entrapment spots	Minimizing isolated areas; avoiding blind spots of buildings and planted areas
	Socio-demographic character	Considering social structure of areas
	Vitality of public spaces	Adequate density and activity; proper land use; human scale
	Well-connected/ integrated plan	Connected streets; proper mixed uses; good street pattern
	Green spaces (urban greenery)	Controlled green spaces and parks
	Proper placement of lighting and security cameras	Good placement of street lighting and security cameras
	Anti-terrorist planning	Anti-terrorism planning for target: a temporary or permanent site or building that is sensitive to terrorism (e.g. fan zone, multi-activity hall type arena, courthouse, government building, headquarters of an iconic company)
Design	Visibility	Landscape; planting; lighting illumination/colour rendering/ uniformity; large glass windows
	Access control	Entry barriers, walls and fences, gates certified by relevant performance standards
	Site/target hardening	Soft target building/street hardening through security equipment (e.g. vehicle security barriers, windows and doors, locks, mesh and grilles) certified by relevant security performance standards
	Territoriality	Clear demarcation of space; sense of ownership/responsibility; buffer zone
	Attractive design	Positive area image; attractive lighting and public art
	Robust materials	Vandal-resistant street furniture; convenient maintenance; integrity of devices used for networks (e.g. data, sensors, energy, water, gas, high pressure steam, air intakes)

Table 1 *(continued)*

Stage	Strategies	Examples
Site and social management	Maintenance	Clean streets and alleys; emptied garbage bins; greenery and vegetation on public land
	Surveillance	Security cameras for vulnerable spots; police/security guards targeted patrols
	Public rules enforcement	No drinking zone signs; substantial enforcement
	Swift repairs	One day fixing policy
	Treating vulnerable groups	Providing shelters for homeless people, alcohol/drug addicts, youths
	Publicity activities	Active communications with the public; preventive messages and rules of conduct for the public

5.2.2 CPTED strategies for planning stage

The organization should:

— choose the scale, function and blending of functions to provide an incentive for liveability, social control, involvement and sense of ownership for CPTED strategies in the planning stage;

— implement planning stage strategies to prevent the existing urban environment from being harmed and, in the case of an emerging threat such as a vehicle bomb threat flexibly adopt this strategy;

— create strategies for the conditions for the formation of social networks and making a new development part of the existing surrounding urban environment as much as possible;

— minimize isolated places and avoid blind/entrapment spots of buildings and planted areas that have low visibility from nearby.

The organization should:

— consider the social structure, such as socio-economic and demographic characters of a site in order to reflect its specific context;

— enhance the vitality of public space for the site by considering active land use, density and (human) scale;

— consider properly connected street segments and integrated land uses (rather than disconnected and segregated patterns);

— consider cautious ecological placement of green spaces and parks for an area;

— consider cautious placement of lighting and, if necessary, security cameras for an area;

— consider anti-terrorism building and landscape planning for particular target sites;

— consider the security and crime prevention of the construction site against attacks (e.g. the misuse of land and building for grouping of offenders, drug trafficking or stolen goods, prostitution, theft of tools, material and building machines, trucks.) during the CPTED planning stage as construction development often lasts for a few years until building completion.

NOTE Table 1 provides additional and detailed information with examples on CPTED strategies for the planning stage.

5.2.3 CPTED strategies for design stage

The organization should:

— evaluate the external and internal situational context of CPTED-related risks;

— understand what factors significantly influence the risk and the effectiveness of countermeasures.

Evaluating the external situational context of the risk includes:

— the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;

— key drivers and trends having an impact on the objectives of the organization;

— relationships with, and the perceptions and values of, external interested parties.

Evaluating the internal situational context of the risk includes:

— governance, organizational structure, roles, responsibilities and accountabilities;

— policies and objectives, and the strategies in place to achieve them;

— capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems, technologies);

— relationships with, and the perceptions and values of, internal interested parties;

— the organization's culture;

— standards, guidelines and models adopted by the internal interested parties.

The organization should aim at creating the conditions for social control, natural surveillance, a sense of ownership and pride in an area for the design stage CPTED strategies.

The organization should integrate the CPTED design strategies as part of the planning and design phase.

The organization should:

— enhance the visibility of streets and buildings by proper building, landscaping and lighting design;

— enhance the access control of a site through gates, fences and walls, or entry/exit barriers tested and certified by relevant security performance standards;

— harden soft target sites/buildings (in addition to traditionally hardened sites) through security equipment certified by relevant security performance standards;

— consider the territoriality of a site by clear demarcation between public space, semi-public space, semi-private space and private space to create buffer zones and to enhance sense of ownership;

— consider the attractiveness/aesthetics of a site in order to create positive area image and active land use by attractive public art and lighting;

— consider clear signage with a proper colour scheme and legibility;

— consider the robustness of street furniture in order to resist vandalism attacks and to facilitate maintenance.

NOTE Table 1 provides additional and detailed information with examples on CPTED strategies for the design stage.

5.2.4 CPTED strategies for site and social management stage

The organization should:

— manage target areas by professional surveillance and maintenance;

— implement the management strategies and support, encourage the natural surveillance and sense of ownership by residents and visitors, and not discourage residents from performing this task;

— assume a certain level of self-regulation, which can be elevated to a higher level with professional support for the management strategy;

— create a complete and effective set of measures for the management strategies.

The organization should:

— keep proper maintenance of a site in order to have a positive image by street cleaning or emptying garbage bins;

— consider enhancing surveillance by placing security cameras or security patrols for a site when necessary;

— consider setting and enforcing rules for vulnerable areas and places;

— repair broken street furniture or lighting in a speedy manner to eliminate the signs of neglect (as per the broken window theory);

— carefully treat vulnerable groups (e.g. homeless people);

— consider launching a publicity campaign and activities with preventive messages and rules of conduct for active risk communication.

NOTE Table 1 provides additional and detailed information with examples on CPTED strategies for the site and social management stage.

6 Process of CPTED implementation

6.1 General

The organization should mandate CPTED as a design standard as part of a continual improvement process for community/site/building security, safety and quality of life, and not just for the installation of security cameras and murals. The organization should implement a step-by-step process involving all relevant interested parties.

The organization should:

— follow the risk management framework given in ISO 31000 to integrate risk management into CPTED activities and programmes;

— develop the framework following clear decision steps to set a strategy, taking into account the responsibilities of all interested parties involved;

— ensure that CPTED strategies are addressed by the multiple interested parties to adequately manage risk through developing partnering arrangements.

NOTE 1 There are many different roles and responsibilities within and between public, private and not-for-profit organizations.

NOTE 2 ISO 22397 provides principles and a process to develop the relationship among organizations in a partnering arrangement.

The process of CPTED is given in Figure 3.

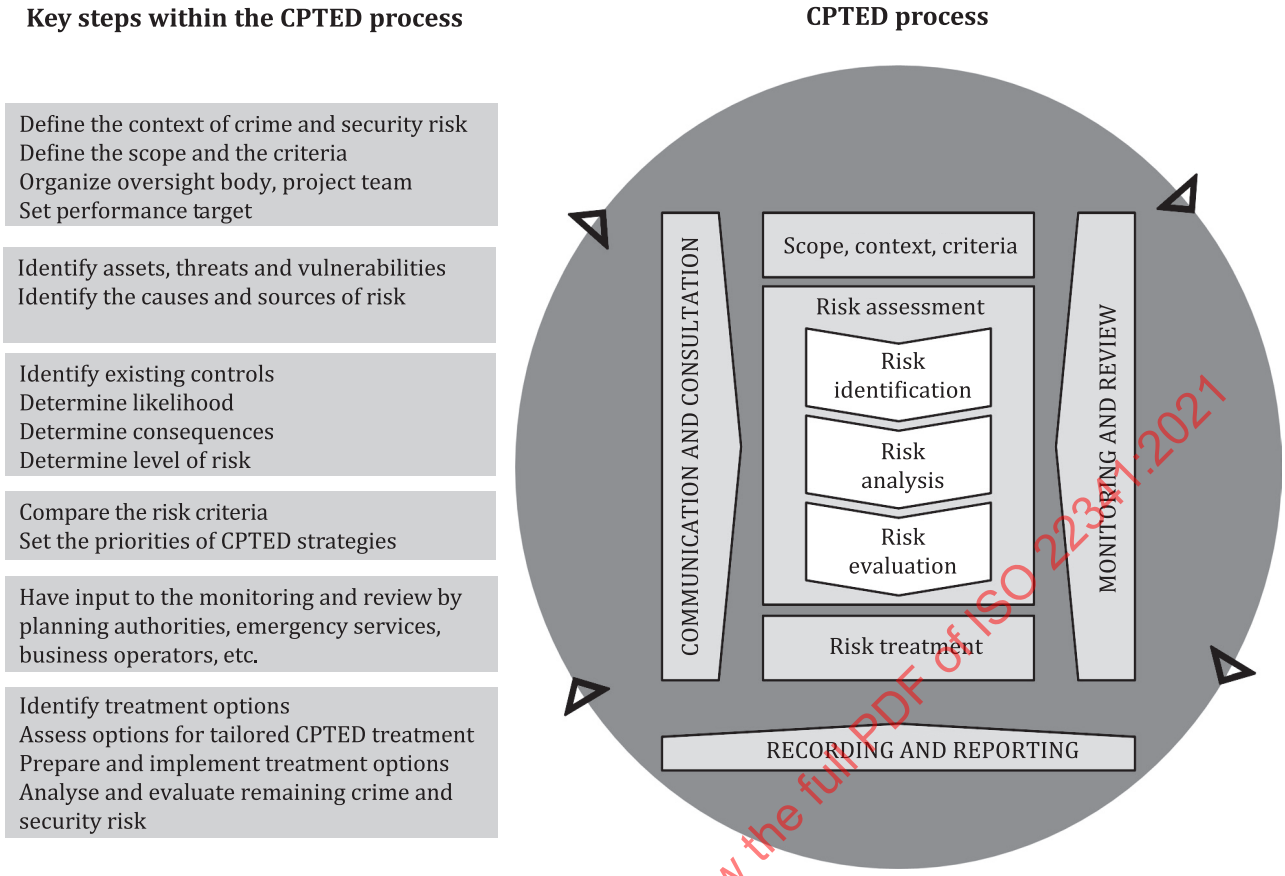

Figure 3 — Process of CPTED

NOTE 3 Depending on practice and theory, there are several other CPTED-related process models, such as the SARA (scanning, analysis, response, assessment) model, which is a commonly used problem-solving method.

The organization should:

— ensure that framework development encompasses integrating, designing, implementing, evaluating and improving risk management across the organization for CPTED leadership and commitment;

— encourage interested parties to initiate a regular planning/management process resulting in the building of a new area or rebuilding, refurbishment or maintenance of an existing area;

— incorporate this document to prevent and reduce crime and the fear of crime in the regular planning/management process;

— define in documented procedures the responsibilities and requirements for planning and conducting evaluation, and for reporting results and maintaining records;

— follow the general principles of CPTED process for continual security improvement for community.

6.2 Oversight body, performance target statement and project team

An authority responsible for granting permission for developments in new and/or existing environments are referred to this document as an “oversight body”. Local or regional authorities may delegate their planning permission responsibilities to another expert group, institute or corporation, in which case the delegated group, institute or corporation will be the oversight body.

The organization should require top management and oversight bodies, where applicable, to ensure that risk management is integrated into all organizational activities and to demonstrate leadership and commitment.

The organization should require the oversight body to provide evidence of its commitment to security and crime prevention/reduction by CPTED by:

— communicating and disseminating the importance of meeting security requirements;

— establishing a security policy;

— conducting a risk assessment in existing or proposed new environments;

— ensuring that general security objectives relate to the relevant rules if they are established;

— defining the areas that are subject to the procedure of this document;

— providing a technical support for security policy;

— ensuring the availability of resources.

The organization should:

— set up a technical structure to support the security policy and crime prevention policy;

— assign to top management the responsibility for starting a process aimed at meeting the security objectives as formulated by the oversight body;

— request the oversight body to appoint a person who, irrespective of other responsibilities, has the responsibility for and authority over:

  — ensuring that the necessary steps in the process are established, implemented and maintained;

  — reporting on the process to other members of the oversight body.

The organization should require that the oversight body confirm that the following four preliminary questions have been answered:

— the exact identification of the area under consideration (where);

— the general identification of the crime problems that can, will or seem to take place in this area (what);

— interested parties (who);

— the identification of strategies and methods (how).

The organization should require the appointed representative of the oversight body to initiate the process for preventing and reducing crime and the fear of crime in a new or existing environment by issuing a performance target statement that includes:

— the main objectives to be pursued for the future security and safety situation within the defined environment;

— the composition of the project team;

— the phases of design and implementation that require evaluations to be carried out;

— general guidance on the organization of the process such as deadlines for each of the identified steps, documentation requirements, resources, technical assistance and relevant laws/regulations.

The organization should ensure that, in accordance with the performance target statement, a multi-disciplinary project team is set up with the representatives of the interested party organizations involved in the particular project. The project team should develop and execute the performance target statement defined by the oversight body. The general tasks include:

— establishing a performance target programme;

— identifying and studying the crime and security problems in the specific area;

— providing guidance to the designers and developers in order to meet the performance target statement;

— providing the oversight body with an evaluation of the extent to which the objectives have been met and how the project is proceeding.

6.3 CPTED process

6.3.1 Step 1 — Communication and consultation

Communication and consultation are important as interested parties make judgements about risk based on their perceptions of risk. These perceptions can vary due to the differences in values, needs, assumptions, concepts and concerns of interested parties. As their views can have a significant impact on the decisions made, the interested parties' perceptions should be identified, recorded and taken into account in the decision-making process.

The organization should:

— communicate and consult with external and internal interested parties during all stages of the risk management process for CPTED projects;

— develop plans for communication and consultation at an early stage;

— address issues relating to the risk, its causes, its consequences and the measures being taken to treat the risk;

— ensure that those accountable for implementing the CPTED process and interested parties understand the basis for decisions, and the reasons why particular preventive actions are required.

The organization should consider a consultative team approach that:

— helps to appropriately establish the context;

— ensures that the interests of interested parties are understood and considered;

— adequately identifies risks;

— brings different areas of expertise together for risk analysis;

— appropriately considers different views when defining risk criteria and evaluating risks;

— secures endorsement and support for a treatment plan;

— enhances appropriate change management during the CPTED process;

— develops an appropriate external and internal communication and consultation plan.

6.3.2 Step 2 — Scope, context and criteria

The organization should:

— define the scope of the process and understanding the external and internal context to customize the management of a specific CPTED project;

— define the scope of its CPTED activities as a risk management process for organizational objectives and performance targets;

— specify the amount and type of risk that it may or may not take, relative to objectives;

— establish risk criteria at the beginning of the risk assessment process, and continually review and amend them, if necessary;

— define criteria to evaluate the significance of risk and to support decision-making processes;

— ensure that the risk criteria reflect the organization's values, objectives and resources and is consistent with policies and statements about risk management;

— define the criteria, taking into consideration the organization's obligations and the views of CPTED interested parties.

The organization should ensure that the oversight body:

— declares objectives, policy, process and procedure, commitment to crime prevention for the community and performance target statement;

— establishes the internal and external context and the risk management context for the objective and performance target;

— organizes the project team for planning, implementation and evaluation of the CPTED projects.

6.3.3 Step 3 — Risk assessment

Risk assessment of crime is the overall systematic process for the identification, analysis and evaluation of crime-related risk in an area.

The organization should conduct the risk assessment for CPTED within the internal and external context of the organization that includes definitions of:

— the nature, type and seriousness of crime problems to be tackled (existing environment) or prevented (new environment);

— the factors of the physical and social environment, the built form and the design features that can directly or indirectly contribute to crime problems.

A risk assessment should be performed after the assets in scope have been formally identified. This first step is critical, since the risk assessment will consider risks to assets of value.

Organizational interested parties are typically owners of organizational assets, and those asset owners are inherently also the owners of risks to those assets. Therefore, the security professional(s) should serve as risk experts and trusted advisors to asset owners in making risk-based decisions about securing them.

The organization should:

— find, recognize and record risks for a project area and site;

— include in the risk identification an assets/threats/vulnerabilities assessment, and consider the causes and sources of risk, as well as criminal events, situations and circumstances;

— determine through the risk analysis the level of risk, comprising both the likelihood of crime occurrence and the consequences of crime events.

NOTE 1 The consequences of crime are tangible loss (e.g. financial expenses, property losses, private security expenditures) and intangible loss (e.g. damage to reputation, impact on societal values and behaviour, fear, pain, lost quality of life), which are generated from crime victimization.

NOTE 2 The analysis of likelihood of crime occurrence is gained from official crime data (e.g. police crime data, police call data). The crime data will generally provide temporal and spatial patterns of crime occurrence in an area.

NOTE 3 An analysis of the consequences of crime is usually available from crime perception survey data.

The organization should analyse relevant risk factors (e.g. socio-economic factors, demographic factors, an area's physical factors) using information gained from corresponding local authorities and from:

— field interviews, community safety audits and focus groups;

— site surveys (visual audit) showing the detailed physical security features of an area;

— spatial analysis software or computational tools that measure the degree of accessibility and surveillance quantitatively for specific risk related to a street segment within a city street network.

The organization should consider developing a checklist for risk assessment.

The organization should consider scoring the likelihood of occurrence with standard linear scaling. In order to provide a better stratification of risk levels, the organization should consider using a modified or weighted scaling system.

The organization should consider scoring severity of consequences with standard linear scaling. In order to provide a better stratification of risk levels, the organization should consider using a modified or weighted scaling system.

NOTE IEC 31010 provides a range of qualitative and quantitative risk assessment techniques that include details on the process of planning, implementing, verifying and validating the use of the assessment techniques.

For the risk evaluation process, the organization should:

— compare the estimated levels of crime and security risk with the risk criteria defined when the context was established;

— use the understanding of the risk obtained in the risk analysis to make decisions about the strategies required for risk control and treatment;

— systematically assess risk to apply CPTED-related risk treatments appropriate to the activities planned for the spaces;

— direct the project team to identify, analyse and evaluate the risk of a target area or site, and to select and define the specific CPTED strategies and measures for the implementation of the CPTED project based upon the result of the risk assessment and in accordance with the performance target statement;

— determine the scaling and assignment of risk levels that best suits its priorities and available resources;

— provide the outcome of risk assessment to CPTED interested parties as information for decision-making about the priorities and choices of CPTED strategies;

— discuss the outcome of the risk assessment with the oversight body.

The organization should consider risk-based CPTED countermeasures.

6.3.4 Step 4 — Risk treatment

Decision-making on CPTED security investment for the risk treatment should involve evaluating how much potential loss (i.e. cost of crime) could be avoided by an investment. The monetary value of the investment should be compared to the monetary value of the risk reduction.

The organization should:

— use the concept of return on security investment (ROSI) calculation, which combines the quantitative risk assessment and the cost of implementing security countermeasures for this risk;

— decide in consultation with the oversight body which CPTED strategies are to be implemented for crime and security risk treatment, and which aspects of the plan are to be elaborated further by the project team if necessary;

— set out these options in a final agreement between all interested parties once a final decision on the CPTED treatment options has been made.

This agreement should identify:

— who does what (responsibility of each party involved);

— time schedule;

— intermediate controls of the planned actions.

NOTE 1 Estimates of the social and economic costs of crime can have an important role in achieving the greatest impact on crime for the money spent. Cost of crime estimates can be used in both appraisal and evaluation of crime reduction policies, such as those in the local government's CPTED programme.

NOTE 2 Cost of crime includes costs imposed on individuals, households, businesses or institutions by crimes they suffer directly (private costs) and wider impacts on society as a whole through, for example, responses to the perceived risk of crime (external costs). The social cost of crime therefore includes both financial costs reflected in expenditure and notional costs reflecting best assessments of the less tangible impacts of crime, such as the emotional and physical impact on victims.

The organization should:

— select the CPTED treatment options in accordance with the organization's objectives, risk criteria and available resources, and where possible first consider preventive countermeasures followed by detective and corrective countermeasures;

— implement the risk treatment options described in the final agreement making each party involved in this agreement responsible for the implementation of its respective actions and keeping the others informed on the progress;

— monitor each implementation phase of treatment to determine whether the safety and security requirements are met.

The oversight body should define the way in which the monitoring is carried out.

The organization should:

— make decision-makers and other interested parties aware of the nature and extent of the remaining risk after risk treatment;

— assess and document the remaining risk;

— accept the remaining risk or where appropriate implement further treatment following a review of monitoring information;

— evaluate the performance of the treatment implemented in respect to its safety and security effects.

An evaluation programme should be planned, taking into consideration the defined status and importance of the frequency and methods. Selection of evaluating experts and conduct of evaluations should ensure objectivity and impartiality of the evaluation process.

In the event of crime problems exceeding the specific requirements in a new environment, or remaining at unacceptable levels in an existing environment, the oversight body should decide upon corrective action, to eliminate the cause of nonconformities in order to prevent recurrence, e.g. take additional crime preventive measures or go on with (further) refurbishment of the area.

6.3.5 Step 5 — Monitoring, review, recording and reporting

The organization should:

— plan monitoring and review management using regular checking or surveillance as part of the CPTED process for risk;

— clearly define responsibilities for monitoring and review;

— ensure that the monitoring and review processes encompasses all aspects of the CPTED process in order to:

  — confirm that controls are effective and efficient in both design and operation;

  — obtain further information to improve risk assessment;

  — analyse learning lessons, changes, trends, successes and failures of CPTED treatments;

  — detect changes in the external and internal context, including changes to risk criteria and the risk itself, which can require revision of risk treatments and priorities;

  — identify emerging risks.

— document the CPTED process and its outcomes, and reports them through the appropriate mechanisms so that decisions concerning the creation, retention and handling of documented information are taken into account.

Reporting should be carried out to enhance the quality of dialogue with CPTED interested parties and to support top management and the oversight body in meeting their responsibilities.

6.4 General principles for CPTED process

6.4.1 General

The organization should:

— follow the principles in ISO 31000:2018, Clause 4 and the general principles for a successful CPTED implementation process in order to be a continual improvement system for community and site security;

— base its CPTED implementation on a proper understanding of the general principles of the CPTED process;

— consider more balanced, cost-effective, evidence-based, ecological and adaptive CPTED process approaches in addition to sustainable and resilient application in principle.

6.4.2 Balanced CPTED concept approach

There are two fields of CPTED concepts: physical and social (second generation). Physical CPTED can often promote or facilitate social CPTED. Social crime prevention efforts sometimes lead to the physical improvement of the community. Both CPTED physical and social concepts should be interactive as much as possible rather than stand-alone.

The organization should:

— consider possible conflicts with other goals and values (apart from crime prevention) to make a balanced set of strategies;

— understand that crime prevention is a part of the whole of a planning, design and management process and cannot be considered in isolation.

NOTE Annex B provides additional information.

6.4.3 Cost-effectiveness

CPTED makes possible designs that offer protection with a minimized use of fortress-type construction, by integrating the concept into the overall design and reducing negative visual impacts.

CPTED approaches should be cost-effective by employing the concepts during the planning, designing or construction stage rather than added at a later date.

Planning applications should be properly controlled and reviewed by public or private security institutions when the relevant development or remodelling is carried out in a high-risk area.

The organization should embed CPTED concepts into the planning and development process through examining relevant documentation.

6.4.4 Sustainability and resilience

The organization should consider the principles of sustainable development, which require a balanced consideration of the social, economic and environmental implications of development activities when CPTED is planned.

The organization should consider the principles of resilient communities, which are to protect and enhance people's lives, secure development gains, foster an investible environment, and drive positive change.

The organization should consider incorporating the principles of sustainability and resiliency into environmental design, or redesigning through environmentally and socially sustainable environmental design.

NOTE ISO 37120 provides a uniform approach to what is measured, and how that measurement is to be undertaken for a holistic and integrated approach to sustainable development and the resilience of communities. The number of property crimes and violent crimes is a core or supporting indicator for sustainable development.

6.4.5 Green environment (ecological) approach

The organization should:

— consider green city concept planning and design for the CPTED process in order to reduce the crime and security risk;

— create a safe environment for residents and enhance their quality of life through investments in green spaces;

— consider community-initiated greening of vacant lots in order to have a greater impact on reducing more serious, violent crimes.

6.4.6 Adaptive application

The organization should continue to be reflective and to strive to evaluate and understand its successes and its failures using CPTED to continually adapt to changes such as:

— increasing development, population densities and population diversity;

— new technologies (green technology, smart city technology, etc.) and products;

— new ways of life and emerging crime problems.

6.4.7 Evidence-based approach

The CPTED evaluation is a facilitator for CPTED as a continual improvement system. Evidence indicates certain land uses and environmental settings can exhibit increased levels of crime linked to their routine activities and can influence crime levels in nearby locations.

The organization should:

— take evidence-based approaches by making evaluation an essential process of CPTED programmes;

— evaluate the effect of CPTED programmes in a valid and reliable manner;

— proportionately prepare in advance the associated budgets of conducting the necessary CPTED assessment or necessary modifications that can be required;

— consider the displacement of crime or diffusion of benefits into the surrounding environment in the evaluation research of CPTED programmes;

— evaluate mixed land uses in terms of the nature of the business, their periods of activity, the nature and frequency of the presence of concerned authorities, etc. to minimize negative influences to adjacent areas.

Annex A
(informative)

Key considerations of CPTED

A.1 Where — Identification of the area

For both serious crime and petty crime, the strongest factor explaining crime (and victimization) risks is urbanization, with crime increasing with the proportion of citizens living in larger cities. Next, low socio-economic status (e.g. low income, education) is significantly associated with higher risks.

Within urbanized areas, security and safety can be improved in existing as well as in new and future environments. An area can be the neighbourhood or environment, ranging from just a few houses or streets to the whole city.

The organization should consider different types and scales of areas:

— public spaces, defined as areas with free access to public use (streets, squares, parks and public gardens etc.);

— neighbourhoods and other suburban, urban and rural sectors (residential areas, city centres, commercial/industrial or offices areas, shopping/retail areas as well as mixed-use areas);

— land use and infrastructure planning.

Specific areas such as schools, leisure centres, public transport and parking facilities, stations, bus stops and parking garages should follow the guidance of this document.

It is important to classify the area under consideration as either a new or existing area. In the case of a new area, only a plan exists. For an existing area, the CPTED options are more limited due to the more extensive changes and costs that are required when compared with a new development.

The consequences of these differences are far reaching:

— new environment (= new project): crime and security risk can only be assessed by using theories or by using experiences and lessons from other neighbourhoods/projects closely resembling the plan for this new environment;

— existing environments: risk can be analysed in real situations by way of, for example, official crime data, victimization surveys, security audits, recording the experiences and opinions of residents, site visits, professionals (police officers, shopkeepers, etc.), observations, interviews with victims and/or offenders.

A.2 What — Identification of the problems

A.2.1 General

Having identified the area, the next question is either:

— what are the crime problems in this area?

— what crime problems may arise in the future in this proposed new area?

The problems that have to be taken into account can be quite different, ranging from the fear of crime to antisocial behaviour to major crimes.

Some factors that influence the security challenge are not linked to the local environment but depend on broader conditions.

The various types of crime and security challenge problems may be subdivided in three categories:

— criminal offences (officially recorded by the police), see A.2.2;

— antisocial behaviour (disorder), see A.2.3;

— the fear of crime, see A.2.4.

In addition to crime, antisocial behaviour and the fear of crime, the problem identification should also investigate the propensity of a place toward attracting crime or generating the fear of crime.

A.2.2 Criminal offences

The following list gives examples for different kinds of offences.

— Burglary includes theft from gardens and trespassing without breaking and entering, and can occur on residential and commercial areas and to cars.

— Street violence relates to assault and robbery (threats of violence or violence against a person), fighting and assault (mob violence as gang fight, vehicle attacks including terrorism, car racing, joyriding, carjacking, etc.), sexual violence or indecent acts, and assault.

— Car crime relates to the theft of/from vehicles and arson, including motorcycles and mopeds.

— Theft relates to shop-lifting, pickpocketing and any theft without the use of violence.

— Criminal damage/serious vandalism relates to the destruction and degradation of equipment or material, and damage to public or private property, such as serious graffiti.

— Arson that occurs on public property and goods (e.g. waste disposal units, schools) or on private property and goods (e.g. letterboxes, underground parking).

A.2.3 Antisocial behaviour

Antisocial behaviour and minor conflicts relate to:

— minor vandalism such as broken windows, destruction of a bus stop and graffiti;

— disturbances and antisocial behaviour with no penal qualification such as neighbour quarrels, gangs gathering with aggressive attitudes, noise pollution, illegitimate uses according to the rules of a place;

— littering, garbage or refuse left outside, urinating, and dirt on private or public property;

— conflicts between activities that potentially lead to illegitimate appropriation (young people over elderly users) or to risks of accidents (conflicts between pedestrians and bikers or pedestrians and vehicles leading to risks of accidents).

A.2.4 Fear of crime

Fear of crime refers to the fear of personally becoming a victim of particular types of crime.

Concern about crime and the degree of fear vary depending on the person (this could be a bad feeling when walking alone at night in the neighbourhood or being afraid to use public transport).

It can also be generated by factors that create a climate of tension or discomfort in the use of a place, such as specific factors such as prostitution or drug abuse, vandalism, bad maintenance or problematic environmental design that creates isolation, lack of surveillance, orientation and alternative routes, and even risks of accidents between users (pedestrians, bikers, vehicles).