INTERNATIONAL WORKSHOP AGREEMENT

IWA 37-2

First edition
2022-10

Safety, security and sustainability of cannabis facilities and operations —

Part 2: Requirements for the secure handling of cannabis and cannabis products

Reference number
IWA 37-2:2022(E)

© ISO 2022



COPYRIGHT PROTECTED DOCUMENT

© ISO 2022

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

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

Published in Switzerland

© ISO 2022 – All rights reserved

Contents

Page

Foreword ... **v**

Introduction ... **vi**

1 Scope ... **1**

2 Normative references ... **2**

3 Terms and definitions ... **2**

4 Risk assessment ... **11**
4.1 General ... 11
4.2 Risk identification ... 12
4.3 Risk analysis ... 12
4.4 Risk evaluation ... 13
4.5 Risk treatment ... 13
4.6 Security risk assessment ... 13
4.7 Selection of risk treatment options ... 14
4.8 Risk acceptance ... 15

5 Physical and technical controls ... **15**
5.1 General ... 15
5.2 Security risk assessment (SRA) ... 16
5.3 Physical controls – Specific requirements ... 17
5.3.1 Outer physical barriers ... 17
5.3.2 Cultivation areas ... 17
5.3.3 Doors/portals ... 17
5.3.4 Areas of protection and/or secure storage areas ... 18
5.3.5 Lighting ... 18
5.3.6 Security film ... 18
5.4 Technical/electronic controls - Specific requirements ... 18
5.4.1 General ... 18
5.4.2 Electronic security systems ... 18
5.4.3 Installation, maintenance, and inspection of the electronic security systems ... 18
5.4.4 Intrusion detection systems ... 18
5.4.5 Access control systems ... 19
5.4.6 Video surveillance systems ... 19
5.5 Cybersecurity controls for operational technology ... 20
5.5.1 General ... 20
5.5.2 Roles and responsibilities ... 21
5.5.3 Cybersecurity risk assessment ... 22

6 Administrative controls ... **23**
6.1 General ... 23
6.1.1 Continual improvement cycle ... 23
6.1.2 Administrative controls table ... 23
6.1.3 Security management policy ... 23
6.1.4 Implementation and operation ... 24
6.1.5 Preparing and implementing risk treatment plans ... 25
6.1.6 Competence training and awareness ... 25
6.2 Traceability system ... 25
6.2.1 General ... 25
6.2.2 General design considerations ... 27
6.2.3 Minimum requirements ... 28
6.2.4 Verification/ mass balance / products reconciliation ... 31
6.2.5 Monitoring ... 31
6.2.6 Key performance indicators ... 31
6.2.7 Audit scheduled ... 31
6.2.8 Review ... 31

© ISO 2022 – All rights reserved

6.3 Security management documentation 31
6.3.1 General 31
6.3.2 Document and data control 32
6.3.3 Operational control 32
6.3.4 Emergency response and security recovery 33
7 Requirements for specific activities 33
7.1 Cultivation 33
7.1.1 Physical and technical/electronic controls for cultivation 33
7.1.2 Administrative controls for cultivation security 33
7.2 Processing 36
7.2.1 Physical controls for processing 36
7.2.2 Technical/Electronic controls for processing 36
7.2.3 Administrative controls for processing 36
7.3 Storage/distribution 40
7.3.1 Physical and technical/electronic controls for storage/distribution 40
7.3.2 Cybersecurity controls for storage/distribution 40
7.3.3 Administrative controls for storage/distribution 40
7.4 Research/Testing laboratory 41
7.4.1 Physical controls for research/testing laboratory 41
7.4.2 Technical/Electronic controls for research/testing laboratory 42
7.4.3 Cybersecurity for research/testing laboratory 43
7.4.4 Administrative controls for research/testing laboratory 44
7.5 Retail/dispensary 46
7.5.1 Physical controls for retail/dispensary 46
7.5.2 Technical/electronic controls for retail/dispensary 47
7.5.3 Cybersecurity controls for retail/dispensary 49
7.5.4 Administrative controls for retail/dispensary 49
7.6 Transportation 50
7.6.1 Physical controls for transportation 50
7.6.2 Technical controls for transportation 52
7.6.3 Administrative controls for transportation 52
Annex A (informative) **Threat and risk assessment checklist and instructions 54**
Annex B (informative) **Administrative controls and minimum required content of security policy 59**
Annex C (informative) **Physical and technical/electronic controls 62**
Bibliography 64

© ISO 2022 – All rights reserved

Foreword

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

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

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

International Workshop Agreement IWA 37 was approved at a series of workshops hosted by the Standards Council of Canada (SCC), in association with Underwriters Laboratories of Canada (ULC), held virtually between December 2020 and June 2021.

A list of all parts in the IWA 37 series can be found on the ISO website.

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.

© ISO 2022 – All rights reserved

Introduction

While cannabis has been fully legalized in Canada and in many states in the USA, it is a new and emerging industry that is moving at a very fast pace in many other parts of the world. While legalization is being deliberated by governments and legislative bodies, companies are creating their own infrastructure in anticipation of legal approval. Meanwhile, government regulators and the societies they serve are grappling with the lack of consistent rules and guidance to deliver safety, security and sustainability of cannabis facilities and operations, while growers and producers use their own judgment on how to establish and operate facilities.

It has become very clear that the global cannabis market is opening up very rapidly. The cannabis product and the industry will become more and more ubiquitous as the global barriers start to lower and come down. If the current trend continues, it is predicted that well over one third of the globe will accommodate cannabis by 2024.

What is unique about this new and emerging industry is that it is coming from an illicit status into decriminalization and evolving into a legitimate burgeoning business. Due to its pioneering status, very little exists in terms of research, studies, historical experience and best practices. Standardization is likewise very slow on the uptake and the cannabis industry remains severely underserved.

There are therefore distinct challenges for the safety, security and sustainability of cannabis facilities and operations, which the IWA 37 series seeks to address as follows:

— Part 1: Requirements for the safety of cannabis buildings, equipment and oil extraction operations;

— Part 2 (this document): Requirements for the secure handling of cannabis and cannabis products;

— Part 3: Good production practices (GPP).

In addition to the requirements for facilities specified in this document, statutory and regulatory requirements and codes can apply.

Supporting material to accompany the IWA 37 series is available at the following website: IWA 37 — Safety, security and sustainability of cannabis facilities and operations.

A list of workshop participants is available from the Standards Council of Canada (SCC).

© ISO 2022 – All rights reserved

Safety, security and sustainability of cannabis facilities and operations —

Part 2:
Requirements for the secure handling of cannabis and cannabis products

1 Scope

This document specifies minimum requirements for the security of sites and facilities that handle cannabis and cannabis products for the purposes of cultivation (indoor and outdoor), processing, storage/distribution, transportation, retail sales, and research and testing, in order to prevent harm and/or unauthorized access to assets including (but not limited to):

— physical assets;

— personnel;

— cannabis and cannabis products;

— records and information.

NOTE Premises covered in this document include indoor and outdoor cultivation, processing/production facilities and retail stores.

The overall security programme and individual security measures addressed in this document incorporate three types:

a) physical controls;

b) technical controls;

c) administrative controls.

This document specifies minimum requirements for general security of cannabis and cannabis products, up to and including:

— physical security design/measures intended to deny, deter, delay, respond to, and recover from unauthorized access;

— design, installation and maintenance of electronic security systems intended to restrict access, detect intrusion and visually monitor/record activity in security-sensitive areas;

— procedural security measures intended to instruct day-to-day security activities, both routine and emergency, across an organization;

— personnel security measures intended to ensure all personnel attending the facility are properly screened, instructed and trained in security awareness;

— the monitoring of the security status of cannabis and cannabis products throughout the product lifecycle, from cultivation to retail sale, including transportation.

This document provides guidelines for:

— the installation, maintenance and inspection of physical and electronic premises security and cybersecurity systems;

© ISO 2022 – All rights reserved

— the implementation of information security governance at organizational level to include policies, procedures, and standards to protect the confidentiality, integrity and availability of records and information.

All requirements in this document are generic and intended to be applicable to all organizations in the cannabis supply chain, regardless of size and/or complexity.

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.

IWA 37-1, *Safety, security and sustainability of cannabis facilities and operations — Part 1: Requirements for the safety of cannabis buildings, equipment and oil extraction operations*

ISO 22005, *Traceability in the feed and food chain — General principles and basic requirements for system design and implementation*

IEC 60839-11-1:2013, *Alarm and electronic security systems — Part 11-1: Electronic access control systems – System and components requirements*

IEC 60839-11-2, *Alarm and electronic security systems — Part 11-2: Electronic access control systems – Application guidelines*

IEC 62368-1, *Audio/video, information and communication technology equipment — Part 1: Safety requirements*

IEC 62676-4, *Video Surveillance Systems for Use in Security Applications — Part 4: Application Guidelines*

ANSI/UL 681, *Standard for Safety Installation and Classification of Burglar and Holdup Alarm Systems*

ANSI/UL 687, *Standard for Safety Burglary-Resistant Safes*

ANSI/UL 827, *Standard for Safety Central-Station Alarm Services*

ASTM D8205, *Standard Guide for Video Surveillance System*

ASTM D8218, *Standard Guide for Intrusion Detection System (IDS)*

CAN/ULC-S301:2018, *Standard for Signal Receiving Centres Configurations and Operations*

CAN/ULC-S302, *Standard for the Installation, Inspection and Testing of Intrusion Alarm Systems*

EN 1143-1, *Secure storage units — Requirements, classification and methods of test for resistance to burglary — Part 1: Safes, ATM safes, strongroom doors and strongrooms*

EN 50518, *Monitoring and alarm receiving centre*

UL 972, *Standard for Safety Burglary Resisting Glazing Material*

3 Terms and definitions

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

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

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

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

© ISO 2022 – All rights reserved

3.1
access control system
system designed to grant to authorized persons, or entities, entry to and/or exit from a security *controlled area* (3.15) and deny such entry and/or exit to non-authorized individuals, or entities

[SOURCE: IEC 60839-11-1:2013, 3.63, modified – Second preferred term "electronic access control system" and Note 1 to entry have been deleted.]

3.2
authority having jurisdiction
AHJ
organization (3.35), office, or individual responsible for enforcing the *requirements* (3.44) of a code or standard, or for approving equipment, materials, an installation, or a procedure

Note 1 to entry: Note to entry: Also referred to as "competent authority".

[SOURCE: ISO 7076-5:2014, 3.4, modified – Note 1 to entry has been added.]

3.3
cannabis
genus of flowering plants made up of many different phytocannabinoids and chemical compounds

Note 1 to entry: Research into cannabis by governing bodies and *organizations* (3.35) is ongoing around the world, and drug classifications are constantly under review. Regulation of cannabis legalization frameworks can vary between jurisdictions, based on the levels of tetrahydrocannabinol (THC) available in the plant.

3.4
cannabis derivative
secondary *product* (3.42) that can be extracted or obtained from a *cannabis* (3.3) biomass

Note 1 to entry: Classification of synthetically derived cannabinoids can vary between jurisdictions.

3.5
cannabis edible
food (3.24) which includes *cannabis* (3.3) or *cannabis derivative* (3.4) as an ingredient

Note 1 to entry: Dried cannabis, fresh cannabis, cannabis plants or cannabis plant seeds are not in themselves considered food.

3.6
cannabis product
packaged goods containing *cannabis* (3.3) or *cannabis derivative* (3.4), available in multiple formats for commercial and/or retail distribution

3.7
cannabis waste
solid, liquid or gaseous material that is a *cannabis product* (3.6), contains *cannabis* (3.3) or has come into contact with cannabis, destined for disposal and not intended for sale or for use in any way other than for agronomic purposes such as compost

Note 1 to entry: Definitions of cannabis waste can vary between jurisdictions. For example, in a jurisdiction that sets a specific tetrahydrocannabinol (THC) threshold to define cannabis waste at a specific concentration of THC (e.g. 10 µg/g), waste that has a concentration below that threshold is not considered to be cannabis waste.

3.8
chain of custody
process (3.41) by which inputs and outputs and associated information are transferred, monitored and controlled as they move through each step in the relevant supply chain

[SOURCE: ISO 22095:2020, 3.1.1]

© ISO 2022 – All rights reserved

3.9
competence
ability to apply knowledge and skills to achieve intended results

[SOURCE: ISO 22000:2018, 3.4]

3.10
complete protection
electronic protection of any point at which entry can be gained without cutting or tearing down any part of the premises structure, in order to detect entry through it, in addition to the detection of the physical removal of any moveable or removable portion of the closure over the opening

3.11
conformity
fulfilment of a *requirement* (3.44)

[SOURCE: ISO 22000:2018, 3.5]

3.12
contamination
introduction or occurrence of a contaminant including a *safety hazard* (3.48) in a *product* (3.42) or processing environment

[SOURCE: ISO 22000:2018, 3.6]

3.13
continual improvement
recurring activity to enhance *performance* (3.37)

[SOURCE: ISO 22000:2018, 3.7]

3.14
control measure
action or activity that is essential to prevent a *safety hazard* (3.48) and/or significant safety hazard or reduce it to an acceptable level

Note 1 to entry: Control measure(s) is (are) identified by *risk* (3.46) assessment/hazard analysis.

[SOURCE: ISO 22000:2018, 3.8, modified — The words “a significant food safety hazard” have been replaced with “a safety hazard and/or significant safety hazard” in the definition; the original Note 1 to entry has been deleted and the words “risk assessment” have been added to the remaining Note to entry.]

3.15
controlled area
room, area, building, premises or parts thereof to which access is monitored, limited, or controlled

3.16
corrective action
action to eliminate the cause of a *nonconformity* (3.32) and to prevent recurrence

Note 1 to entry: There can be more than one cause for a nonconformity.

Note 2 to entry: Corrective action includes cause analysis.

[SOURCE: ISO 22000:2018, 3.10]

3.17
cultivation
process (3.41) of growing *cannabis* (3.3), including drying, trimming, milling and storing

© ISO 2022 – All rights reserved

3.18
documented information
information required to be controlled and maintained by an *organization* (3.35) and the medium on which it is contained

Note 1 to entry: Documented information can be in any format and media, and from any source.

Note 2 to entry: Documented information can refer to:

— the *management system* (3.30), including related processes;

— information created in order for the organization to operate (documentation);

— evidence of results achieved (records).

[SOURCE: ISO 22000:2018, 3.13]

3.19
duress alarm
silent alarm signal generated by the manual entry of a designated code at the system keypad in the event that the user needs assistance, such as when being forced to disarm the burglar alarm system against the user's will to enter the premises

Note 1 to entry: A duress alarm can also be referred to as an ambush alarm or a panic alarm

Note 2 to entry: Duress alarms are typically treated as *holdup alarms* (3.24) by *monitoring* (3.31) station personnel and are dispatched upon immediately without the need for any type of alarm *verification* (3.55).

3.20
effectiveness
extent to which planned activities are realized and planned results achieved

[SOURCE: ISO 22000:2018, 3.14]

3.21
electronic security system
electronic system or combination of systems that monitor(s) or control(s) activity at a premises, including alarm, access control, video surveillance and unmanned vehicle systems

3.22
extent of protection
designation used to describe the amount of electronic protection installed at a designated area (e.g. *complete protection* (3.10), partial protection)

3.23
extraction
process (3.41) where a substance is removed or separated from other compounds, a solution or a mixture

3.24
food
substance (ingredient), whether processed, semi-processed or raw, which is intended for consumption, and includes drink, chewing gum and any substance which has been used in the manufacture, preparation or treatment of "food" but does not include cosmetics or tobacco or substances (ingredients) used only as drugs

[SOURCE: ISO 22000:2018, 3.18, modified — The original Note to entry has been deleted.]

3.25
greenhouse
building that can have unlimited size, and with more than 50 % of surface area of roofs and/or walls being transparent and/or translucent for the *cultivation* (3.17) of *cannabis* (3.3) plants and other cultivation activities

© ISO 2022 – All rights reserved

3.26
grow area
area of the site where *cannabis* (3.3) plants are cultivated, harvested or propagated

3.27
holdup alarm
alarm initiated by an individual who perceives a threat to the *safety* (3.47) and/or security of persons, facilities, or vehicles, or of being coerced

Note 1 to entry: The alarm is typically silent, but can be visible, and/or audible.

Note 2 to entry: The signalling device can be covert or overt.

3.28
interested party
person or *organization* (3.35) that can affect, be affected by, or perceive itself to be affected by a decision or activity

[SOURCE: ISO 22000:2018, 3.23, modified — The admitted term “stakeholder” has been deleted.]

3.29
lot
defined quantity of a *product* (3.42) produced and/or processed and/or packaged essentially under the same conditions

Note 1 to entry: The lot is determined by parameters established beforehand by the *organization* (3.35) and may be described by other terms, e.g. batch.

Note 2 to entry: The lot may be reduced to a single unit of product.

[SOURCE: ISO 22000:2018, 3.24]

3.30
management system
set of interrelated or interacting elements of an *organization* (3.35) to establish *policies* (3.39) and *objectives* (3.33) and *processes* (3.41) to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines.

Note 2 to entry: The system elements include the organization's structure, roles and responsibilities, planning and operation.

Note 3 to entry: The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

Note 4 to entry: Relevant disciplines are, for example, a quality management system or an environmental management system.

[SOURCE: ISO 22000:2018, 3.25]

3.31
monitoring
determining the status of a system, a *process* (3.41) or an activity

Note 1 to entry: To determine the status, there may be a need to check, supervise or critically observe.

Note 2 to entry: In the context of *cannabis* (3.3) *safety* (3.47), monitoring is conducting a planned sequence of observations or measurements to assess whether a process is operating as intended.

Note 3 to entry: Distinctions are made in this document between the terms *validation* (3.54), monitoring and *verification* (3.55):

© ISO 2022 – All rights reserved

— validation is applied prior to an activity and provides information about the capability to deliver intended results;

— monitoring is applied during an activity and provides information for action within a specified time frame;

— verification is applied after an activity and provides information for confirmation of *conformity* (3.11).

[SOURCE: ISO 22000:2018, 3.27, modified — The words "food safety" have been replaced with "cannabis safety" in Note 2 to entry.]

3.32
nonconformity
non-fulfilment of a *requirement* (3.44)

[SOURCE: ISO 22000:2018, 3.28]

3.33
objective
result to be achieved

Note 1 to entry: An objective can be strategic, tactical, or operational.

Note 2 to entry: Objectives can relate to different disciplines (such as financial, health and *safety* (3.47), and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, *product* (3.42), and *process* (3.41).

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as a food safety *management system* (3.30) objective, or by the use of other words with similar meaning (e.g. aim, goal, or target).

Note 4 to entry: In the context of food safety management systems, objectives are set by the *organization* (3.35), consistent with the food safety *policy* (3.39), to achieve specific results.

[SOURCE: ISO 22000:2018, 3.29]

3.34
operational technology
OT
hardware and software that detects or causes a change through the direct *monitoring* (3.31) and/or control of physical devices and systems, *processes* (3.41), and events in an *organization* (3.35)

3.35
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* (3.33)

Note 1 to entry: The concept of organization includes, but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

[SOURCE: ISO 22000:2018, 3.31]

3.36
outsource
make an arrangement where an external *organization* (3.35) performs part of an organization's function or *process* (3.41)

Note 1 to entry: An external organization is outside the scope of the *management system* (3.30), although the outsourced function or process is within the scope.

[SOURCE: ISO 22000:2018, 3.32]

© ISO 2022 – All rights reserved

3.37
performance
measurable result

Note 1 to entry: Performance can relate either to quantitative or qualitative findings.

Note 2 to entry: Performance can relate to the management of activities, *processes* (3.41), *products* (3.42) (including services), systems or *organizations* (3.35).

[SOURCE: ISO 22000:2018, 3.33]

3.38
physical security
security measures that are designed to deny access to unauthorized persons from physically accessing a building, premises, secured area or security container

3.39
policy
intentions and direction of an *organization* (3.35) as formally expressed by its *top management* (3.52)

[SOURCE: ISO 22000:2018, 3.34]

3.40
potency
amount per unit of the standardized component(s) which further characterizes the quantity of the ingredient

Note 1 to entry: The use of the term potency in this document is not intended to refer to *product* (3.42) efficacy.

3.41
process
set of interrelated or interacting activities which transforms inputs to outputs

[SOURCE: ISO 22000:2018, 3.36]

3.42
product
output that is a result of a *process* (3.41)

Note 1 to entry: A product can be a service.

[SOURCE: ISO 22000:2018, 3.37]

3.43
protected area
protected premises, or an area within, that is provided with means to prevent an unwanted event

Note 1 to entry: Protected areas are imposed in the low security level.

3.44
requirement
need or expectation that is stated, generally implied or obligatory

Note 1 to entry: "Generally implied" means that it is custom or common practice for the *organization* (3.35) and *interested parties* (3.28) that the need or expectation under consideration is implied.

Note 2 to entry: A specified requirement is one that is stated, for example in *documented information* (3.18).

[SOURCE: ISO 22000:2018, 3.38]

© ISO 2022 – All rights reserved

3.45
restricted area
room, area, or building within a site for which access is only permitted for authorized persons

Note 1 to entry: Restricted areas are imposed in the high security level.

[SOURCE: IEC 62128-1:2013, 3.9.5, modified – The word "area" has been replaced with "room, area, or building within a site" and Note 1 to entry has been added.]

3.46
risk
effect of uncertainty

Note 1 to entry: An effect is a deviation from the expected – positive or negative.

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

Note 3 to entry: Risk is often characterized by reference to potential "events" (as defined in ISO Guide 73:2009, 3.5.1.3) and "consequences" as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated "likelihood" (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence.

[SOURCE: ISO 22000:2018, 3.39, modified — The original Note 5 to entry has been deleted.]

3.47
safety
assurance that the *product* (3.42) will not cause an adverse health effect for the consumer when it is prepared and/or used according to its intended use

Note 1 to entry: Safety is related to the occurrence of *safety hazards* (3.48) in end products and does not include other health aspects.

3.48
safety hazard
source or situation with the potential to cause an adverse health effect

Note 1 to entry: The term hazard is not to be confused with the term *risk* (3.46) which, in the context of *safety* (3.47), means a function of the probability of an adverse health effect (e.g. becoming diseased) and the severity of that effect (e.g. death, hospitalization) when exposed to a specified hazard.

Note 2 to entry: Safety hazards include allergens and radiological substances.

[SOURCE: ISO 22000:2018, 3.22, modified — The word "food" has been deleted from the term and from Notes 1 and 2 to entry; the words "biological, chemical or physical agent in food" have been replaced with "source or situation" in the definition; the original Notes 3 and 4 to entry have been deleted.]

3.49
secure area
area with defined physical perimeters and barriers, with physical entry controls or access point protection or access point observation

Note 1 to entry: Secure areas are imposed in the medium security level.

[SOURCE: IEC 61162-460:2018, 3.37, modified – The original Note 1 to entry has been deleted and a new Note 1 to entry has been added.]

3.50
security risk assessment
overall *process* (3.41) of identification, analysis and evaluation of *risks* (3.46) to security *objectives* (3.33) and outcomes

© ISO 2022 – All rights reserved

3.51
signal receiving centre
SRC
portion, or portions of a building, occupied by the alarm operating company, which encompasses the centre operations area and the facilities essential to the operation of *monitoring* (3.31), processing, and disposition of alarm signals

[SOURCE: CAN/ULC-S301:2018, 3.13]

3.52
top management
person or group of people who directs and controls an *organization* (3.35) at the highest level

Note 1 to entry: Top management has the power to delegate authority and provide resources within the organization.

Note 2 to entry: If the scope of the *management system* (3.30) covers only part of an organization, then top management refers to those who direct and control that part of the organization.

[SOURCE: ISO 22000:2018, 3.41]

3.53
traceability
ability to follow the history, application, movement and location of an object through specified stage(s) of production, processing and distribution

Note 1 to entry: Movement can relate to the origin of the materials, processing history or distribution of the *product* (3.42).

Note 2 to entry: An object can be a product, a material, a unit, equipment, a service, etc.

[SOURCE: ISO 22000:2018, 3.42, modified — The word “food” has been replaced with “product” in Note 1 to entry.]

3.54
validation
obtaining evidence that a *control measure* (3.14) (or combination of control measures) will be capable of effectively controlling the significant *safety hazard* (3.48)

Note 1 to entry: Validation is performed at the time a control measure combination is designed, or whenever changes are made to the implemented control measures.

Note 2 to entry: Distinctions are made in this document between the terms validation, *monitoring* (3.31) and *verification* (3.55):

— validation is applied prior to an activity and provides information about the capability to deliver intended results;

— monitoring is applied during an activity and provides information for action within a specified time frame;

— verification is applied after an activity and provides information for confirmation of *conformity* (3.11).

[SOURCE: ISO 22000:2018, 3.43, modified — The word “food” has been deleted from the definition.]

3.55
verification
confirmation, through the provision of objective evidence, that specified *requirements* (3.44) have been fulfilled

Note 1 to entry: Distinctions are made in this document between the terms *validation* (3.54), *monitoring* (3.31) and verification:

— validation is applied prior to an activity and provides information about the capability to deliver intended results;

© ISO 2022 – All rights reserved

— monitoring is applied during an activity and provides information for action within a specified time frame;

— verification is applied after an activity and provides information for confirmation of *conformity* (3.11).

[SOURCE: ISO 22000:2018, 3.45]

3.56
video surveillance system
video surveillance system based on an IP video network used within a protected site

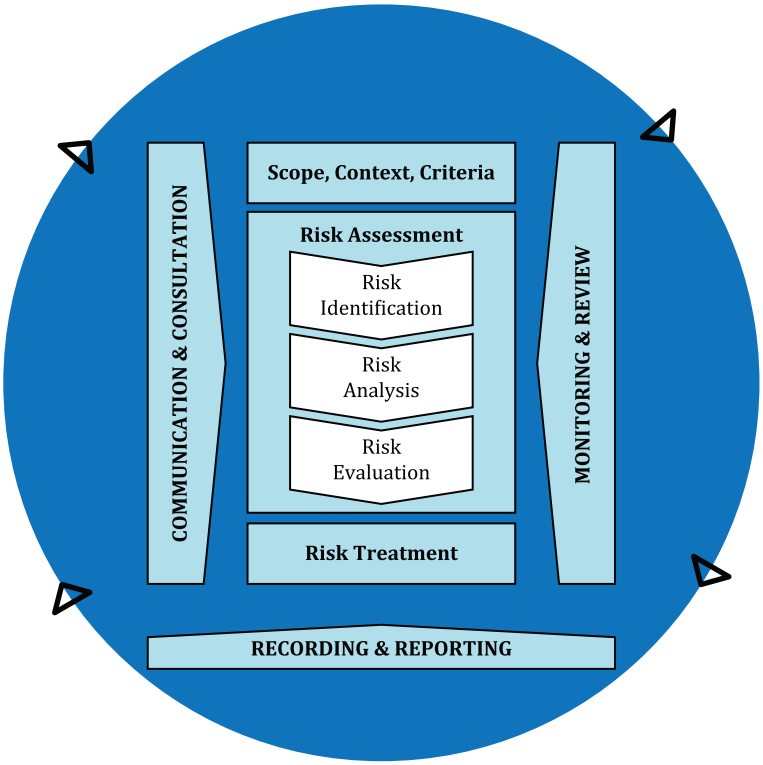
Note 1 to entry: A video surveillance system can consist of closed-circuit television (CCTV) systems and digital imaging devices, *monitoring* (3.31) and recording devices designed to provide visual identification of a person, object or scene in the areas being monitored.

[SOURCE: IEC 62676-2-1:2013, 3.1.64, modified – The original terms "video surveillance system network" and "VSS network" have been replaced with "video surveillance system" and Note 1 to entry has been added.]

4 Risk assessment

4.1 General

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation. See Figure 1.



SOURCE: ISO 31000:2018, Figure 4.

Figure 1 — Risk assessment process

Risk assessment should be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of interested parties. It should use the best available information, supplemented by further enquiry as necessary.

© ISO 2022 – All rights reserved