

ICS 13.310

English version

Guidelines for the evaluation of installed security systems, based on the STEFi dimensions

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN-CENELEC Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

European foreword.....	3
Introduction	5
1 Scope.....	7
2 Terms and definitions	7
2.1 Methodology	7
2.2 STEFi criteria and sub-criteria	11
3 The methodology.....	14
3.1 General.....	14
3.2 The four dimensions	15
3.2.1 Introduction	15
3.2.2 The Security Dimension.....	16
3.2.3 The Trust Dimension	17
3.2.4 The Efficiency Dimension.....	17
3.2.5 The Freedom Infringement Dimension.....	18
4 Parties involved in the methodology, including their roles and responsibilities	18
5 The evaluation.....	20
5.1 Introduction.....	20
5.2 Roles and responsibilities.....	20
5.3 Competencies of the parties involved.....	21
5.4 Conducting the evaluation	23
5.4.1 Configuration (selection and determination).....	23
5.4.2 Assessment of the security system using STEFi criteria	25
5.4.3 Identification and determination of conflicts.....	25
6 Certification.....	29
Annex A (informative) STEFi assessment questions and requirements for video surveillance systems.....	30
Annex B (informative) Standards specifying requirements for the evaluation process.....	55

European foreword

CWA 17147:2017 was developed in accordance with CEN-CENELEC Guide 29 “CEN/CENELEC Workshop Agreements – The way to rapid agreement” and with the relevant provisions of CEN/CENELEC Internal Regulations - Part 2. It was agreed on 2017-03-30 in a Workshop by representatives of interested parties, approved and supported by CEN following a public call for participation made on 2016-09-13. It does not necessarily reflect the views of all stakeholders that might have an interest in its subject matter.

The final text of CWA 17147:2017 was submitted to CEN for publication on 2017-04-07. It was developed and approved by:

1. European Association for the Co-ordination of Consumer Representation in Standardisation (ANEC)
2. Belgian Association for Non Destructive Testing (BANT)
3. Ductis GmbH
4. Euralarm
5. Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. (by participation of Dr. Erik Krempel)
6. Garante per la protezione dei dati personali (GPDP)
7. Information Commissioner of the Republic of Slovenia
8. LINK GmbH
9. Nederlands normalisatie-instituut NEN
10. Slovenian Institute of Quality and Metrology (SIQ)
11. Technological Educational Institute of Central Macedonia, Serres, Greece
12. Technische Universität Berlin – Zentrum Technik und Gesellschaft/Center for technology and Society (CTS)
13. Technische Universität Berlin – Fachgebiet Innovation Economics (INNO)
14. Trilateral Research
15. Universitat Jaume I de Castellon
16. VICESSE
17. Vrije Universiteit Brussel (VUB)

It is possible that some elements of CWA 17147:2017 may be subject to patent rights. The CEN-CENELEC policy on patent rights is set out in CEN-CENELEC Guide 8 “Guidelines for Implementation of the Common IPR Policy on Patents (and other statutory intellectual property rights based on inventions)”. CEN shall not be held responsible for identifying any or all such patent rights.

The Workshop participants have made every effort to ensure the reliability and accuracy of the technical and non-technical content of CWA 17147:2017, but this does not guarantee, either explicitly or implicitly, its correctness. Users of CWA 17147:2017 should be aware that neither the Workshop participants, nor CEN can be held liable for damages or losses of any kind whatsoever which may arise from its application. Users of CWA 17147:2017 do so on their own responsibility and at their own risk.

Introduction

This CWA is based on the results of CRISP (Evaluation and Certification Schemes for Security Products)¹ that was a research project funded by the European Commission². The aim of that project was to develop an innovative evaluation and certification methodology for security systems. The results of this project together with this CWA will be used to establish a certification scheme that will:

- contribute to measures that increase citizen trust and confidence in security technologies through the evaluation of social and legal impacts of security systems as a basis for certification of these systems;
- promote that the use of security systems is based on demonstrated evidence of their security effects and societal impacts;
- enhance dialogue and co-operation between the various stakeholders involved in the operation of security systems in a specific context;
- facilitate a more harmonized playing field for the European security industry by providing pan-European certification for security systems. The aim is to get this scheme accepted across Europe, which would enhance competitiveness by reducing commercialisation costs for the industry;
- support the goal to provide security in an efficient manner.

The innovative part of the methodology for the evaluation of security systems described in this CWA is the assessment of systems from the perspective of four different, though interrelated dimensions:

- a) **security** (the functionality and effectiveness of a security system in identifying and mitigating threats and reducing risks related to e.g. accuracy, circumvention, robustness, system interference and performance);
- b) **trust** (experiences and perceptions of the users of security systems in regard to their actual performance, both employees and persons subject to scrutiny related to e.g. availability, usability, reliability, system integrity, transparency, and accountability);
- c) **efficiency** (economic dimension of the security system related to e.g. the product life cycle costs, such as the purchasing costs, the implementation costs, the operating costs, throughput);
- d) **freedom infringement** (impact of security systems on the freedoms and rights of persons, related to e.g. enhanced personal data collection, processing, and retention, due process, complaint mechanisms).

These dimensions are referred to as the STEFi dimensions (**S**ecurity, **T**rust, **E**fficiency and **F**reedom **i**nfringement) and the methodology integrates these in its evaluation phase. This is an innovative approach as certification has, to date, primarily focused on the evaluation of technical requirements for security systems (the security dimension) or singled out other relevant dimensions (e.g. privacy or data protection in the freedom infringement dimension). The methodology described in this CWA, however, is not (over)simplifying the complexity of assessing security systems but acknowledges and addresses this complexity by identifying potential conflicts between the various assessment dimensions and

¹ www.crispproject.eu

² This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607941.

related criteria and by providing an approach to resolve these conflicts in specific situations. The methodology does not single out technical, legal, social or economic aspects, but integrates these in a multidimensional and multi-stakeholder assessment. This novel concept to integrate different dimensions of security systems in a single evaluation and certification methodology will first be piloted for video surveillance systems, to test and refine the STEFi approach. It is foreseen that the methodology and the future certification scheme in which it will be applied can be extended to include other types of security systems. The combination of evaluation and certification of systems is based on the widely accepted functional approach to conformity assessment as described in ISO/IEC 17000 and implemented in conformity assessment of products as specified in ISO/IEC 17065 and ISO/IEC 17067.

The methodology described in this CWA will serve as the basis for a certification scheme that will be developed after finalization of the CRISP project. The future scheme will not redefine the technical requirements that are already included in e.g. European and international standards or existing certification schemes. The future scheme is intended to contribute to the protection of fundamental rights and promote compliance with relevant EU laws, with a particular focus on the General Data Protection Regulation (GDPR) 679/2016³, by including social, legal and economic requirements in the evaluation and certification of security systems. Certification according to this scheme is initially intended for organizations that install video surveillance systems in a specific context and organizations that procure or employ these systems on their premises.

3 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

1 Scope

This workshop agreement describes the methodology for the evaluation of security systems that are or will be applied in a specific context, applying the STEFi approach. The evaluation involves application of STEFi criteria in four dimensions, namely security, trust, efficiency and freedom infringement. These criteria are not only applied individually but also their interrelationships are taken into account and the STEFi approach thus provides a holistic view on the aspects and impacts of security systems. The aim is that the evaluation process described in this CWA will provide reproducible results; i.e. different evaluation bodies that apply the methodology to similar systems in a similar context, should reach similar conclusions.

NOTE 1 It will be part of the management and maintenance of the future certification scheme to enhance reproducibility of results of STEFi evaluation, e.g. by exchange and discussion of experiences, discussing case studies as a basis for further refining the requirements for the evaluation method.

While the methodology that is described in this CWA is generally applicable to all types of security systems, the examples given and the list of assessment questions and requirements in Annex A are specifically related to planned and installed video-surveillance systems in a specific context.

NOTE 2 Application of the video-surveillance systems in specific context implies that the system is already installed or designed and to be installed in specific and already known situations. This is a boundary condition, because otherwise full application of the STEFi evaluation is not possible.

The overall goal of the CWA is to provide a basis for including the STEFi approach for the evaluation of security systems in a certification scheme. The CWA excludes the certification scheme itself. The target group of this CWA are organizations that deal with evaluation of security systems and that are willing to enhance the scope of their evaluation in order to take into account the overall societal impact of these systems.

The methodology is applicable to security systems in a specific context (i.e. installed or planned to be installed). A system is defined as a set of interrelated or interacting components. Individual components of security systems can be certified separately against applicable technical and other relevant standards; if so, it shall be taken into account as evidence for conforming with specific STEFi criteria.

2 Terms and definitions

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

2.1 Methodology

2.1.1

assessment question

question for assessing a **security system** (2.1.20) in the **evaluation phase** (2.1.13)

Note 1 to entry: The assessment question can either be a yes/no question or a question requesting a qualitative answer.

2.1.2

assessment requirement

requirement to be met by a **client** (2.1.7) and/or a **security system** (2.1.20) that is assessed by a certification body during the **certification phase** (2.1.6) as a basis for the certification decision

Note 1 to entry: Assessment requirements are related to **assessment questions** (2.1.1)

2.1.3

assessment stage

stage of the **evaluation phase** (2.1.13) in which a **security system** (2.1.20) is evaluated by using the **assessment questions** (2.1.1)

2.1.4

certification

third-party attestation related to products, processes, systems or persons

Note 1 to entry: Attestation is the issuance of a statement, based on a decision following review that fulfilment of specified requirements has been demonstrated.

2.1.5

certification body

body that performs **certification** (2.1.4)

2.1.6

certification phase

review of the **evaluation phase** (2.1.13) and its results and assessment of a **security system** (2.1.20) against applicable **assessment requirements** (2.1.2)

2.1.7

client

individual or organisation that is applying for **certification** (2.1.4)

Note 1 to entry: The client usually will be the operator of a security system. The client can also be the organization that designs and installs the security system in a specific context on behalf of the operator.

Note 2 to entry: The client is responsible to the certification body for ensuring that the applicable certification requirements are fulfilled.

2.1.8

configuration stage

stage of the evaluation phase in which general and specific information on a **security system** (2.1.20) is provided by a **client** (2.1.7) and third parties as **information providers** (2.1.14)

2.1.9

conflict

situation where results of the yes/no answers of the **assessment questions** (2.1.1) lead to conflicting requirements for the client and/or a **security system** (2.1.20)

2.1.10 end-user

person or organisation that utilises/operates a **security system** (2.1.20)

EXAMPLE staff member, consumer, scrutinised.

2.1.11 evaluation

systematic examination of a security system (2.1.20) from the perspective of the four STEFi dimensions

2.1.12 evaluation body

body that performs **evaluation** (2.1.11)

2.1.13 evaluation phase

assessment of a **security system** (2.1.20) on the basis of **assessment questions** (2.1.1) aimed at identification of any potential **conflicts** (2.1.9)

Note 1 to entry: The evaluation phase consists of the configuration stage and the assessment stage.

2.1.14 information provider

internal or external independent expert who is familiar with a **security system** (2.1.20) which is assessed and can be involved to assist in answering assessment questions

2.1.15 project leader

person that manages the overall process of the **evaluation phase** (2.1.13) on behalf of the evaluation body

2.1.16 scenario

qualitative description of a series of events in time and space and their inter-relationships related to the operation of a **security system** (2.1.20)

2.1.17 scrutinised

individual, group or organisation that might be affected by, or perceive itself to be affected by a **security system** (2.1.20)

2.1.18 security

condition (perceived or confirmed) of being protected against risks, threats, hazards, loss or any other (man-made) detrimental incidents

Note 1 to entry: "Security" means not only that something is secure, but that it has been secured.

Note 2 to entry: This definition is adapted from ISO/DIS 34001.

2.1.19

security function

intended **security** (2.1.18) specific outcome, or aim, of a **security system** (2.1.20) in operation

2.1.20

security system

system (2.1.26) with one or more **security functions** (2.1.19)

2.1.21

STEFi approach

methodology for assessing **security systems** (2.1.20) two levels of criteria in different so-called **STEFi dimensions** (2.1.24): **STEFi criteria** (2.1.22) and the **STEFi sub-criteria** (2.1.23)

Note 1 to entry: STEFi is the abbreviation for Security, Trust, Efficiency and Freedom infringement.

2.1.22

STEFi criteria

first level criteria of the **STEFi approach** (2.1.21), categorising the **STEFi sub-criteria** (2.1.23)

EXAMPLE Accuracy, Transparency, Interoperability, Due process.

2.1.23

STEFi sub-criteria

second level criteria of the **STEFi approach** (2.1.21) leading to the specific **assessment questions** (2.1.1)

EXAMPLE Response time, User protection, Ergonomics, Visibility.

2.1.24

STEFi dimension

category of criteria applied in the **STEFi approach** (2.1.21) related to specific aspects and stakeholder perspectives

Note 1 to entry: The application of the four dimensions should ensure that all relevant aspects and stakeholder perspectives are addressed during the assessment process.

EXAMPLE Security, Trust, Efficiency, Freedom infringement.

2.1.25

STEFi expert

expert who is selected and appointed by the **evaluation body** (2.1.12) and has knowledge and experience in one or more of the **STEFi dimensions** (2.1.24) in order to assess the **security system** (2.1.20) in those dimensions during the **evaluation phase** (2.1.13)

2.1.26

system

set of interrelated or interacting elements in a defined context

Note 1 to entry: The definition is adapted from ISO 9000:2015

Note 2 to entry: Elements of a system may be natural or man-made material objects, as well as modes of thinking and the results thereof (e.g. forms of organization, mathematical methods, programming languages).

2.1.27

video surveillance system

surveillance system comprised of cameras, recorders, interconnections and displays that are used to monitor activities in a store, a company or more generally a specific infrastructure and/or a public place

[ISO 22300:2012, definition 2.6.2]

2.2 STEFi criteria and sub-criteria

2.2.1

accountability

property that ensures that the actions of an entity may be traced uniquely to that entity

2.2.2

accuracy

closeness of a measurement or a result to the reference/true value

Note 1 to entry: This definition is adapted from ISO 5725-1:1994; definition 3.6.

2.2.3

accuracy of data

condition of having correct and up-to-date personal data

2.2.4

awareness

understanding of a situation or subject at the present time based on information or experience

2.2.5

customisation

modification of components of a system to suit a particular individual or task

2.2.6

discrimination

the different treatment of someone solely because of his or her race or ethnicity, gender, religion or belief, disability, age or sexual orientation

Note 1 to entry: This includes also indirect discrimination, i.e. where a rule or practice which seems neutral in fact has a particularly disadvantageous impact upon a person or a group of persons having a specific characteristic.

Note 2 to entry: This definition is derived from Council Directive 2000/78/EC and Council Directive 2000/43/EC.

2.2.7

documentation

(related to the system) paperwork (or other media) prepared during the design, installation and hand over of the system recording details of a **security system** (2.1.20)

Note 1 to entry: Component documentation may be provided by the manufacturer on paper or an alternative medium.

Note 2 to entry: This definition is adapted from IEC 62676-1-1:2014; definition 3.1.46.

2.2.8

due process

fairness in proceedings, in accordance with established and sanctioned principles

2.2.9

environment

circumstances, objects and/or conditions surrounding a **security system** (2.1.20)

2.2.10

ergonomics

parts of qualities of the design of a **security system** (2.1.20) that make it easy to use

2.2.11

interoperability

ability of two or more components or systems to work together

2.2.12

invasiveness (physiological)

intrusion to the physical sphere of the **scrutinised** (2.1.17)

2.2.13

lifecycle costs

expenditure incurred on, or attributable to, a given product throughout its life cycle

Note 1 to entry: Cost is expressed in terms of money expended by one or more stakeholders.

2.2.14**maintenance**

retaining or restoring a component and/or system in an operable condition

2.2.15**operational requirement**

key document for system designers, which clearly defines the operational parameters of a **security system** (2.1.20) according to the agreed expectations

Note 1 to entry: Adapted from IEC 62676-1-1:2014; definition 3.1.100.

2.2.16**performance**

quality with which the intended functions of the equipment are accomplished

2.2.17**personal data**

any information relating to an identified or identifiable natural person

2.2.18**reliability**

ability of a system or product to perform a required function under given conditions for a given time interval

2.2.19**resilience**

adaptive capacity of an organization in a complex and changing environment

[ISO Guide 73:2009; 3.8.1.7]

2.2.20**risk**

combination of the probability of occurrence of harm and the severity of that harm

Note 1 to entry: The probability of occurrence includes the exposure to a hazardous situation, the occurrence of a hazardous event and the possibility to avoid or limit the harm.

[ISO/IEC Guide 51:2014; 3.9]

2.2.21**robustness**

ability of a **security system** (2.1.20) to handle (and recover from) abnormal situations

2.2.22**safety**

condition (perceived or confirmed) of being protected against unintended natural and/or man-made risks, threats, hazards, loss or any other detrimental incidents

2.2.23

transparency

quality of being clear, open and frank

2.2.24

usability

extent to which a **security system** (2.1.20) can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use

Note 1 to entry: This definition is adapted from ISO/DIS 9241-11.2; 3.1.1.

3 The methodology

3.1 General

The methodology includes a new approach for the evaluation and certification of security systems by integrating the STEFi dimensions into a single evaluation. The methodology follows the widely accepted functional approach to conformity assessment (see e.g. ISO/IEC 17067) of products and is divided in two subsequent phases:

- 1) an evaluation phase comprising two main stages (configuration including reporting, STEFi assessment including reporting);
- 2) a certification phase, consisting of three stages (audit, attestation and surveillance including reporting).

In the evaluation phase the STEFi approach is applied during the assessment stage, on the basis of assessment questions. The approach includes a three level structure consisting of the STEFi dimensions (level one) which are divided into STEFi criteria (level two) which are further sub-divided into sub-criteria (level three) that are translated into assessment questions.

In the evaluation phase information and evidence is first gathered for each assessment question individually. On the basis of this information and evidence conflicts are identified, i.e. conflicting criteria (and the related assessment requirements) for the security system within and between the four dimensions. The outcome of the evaluation is a report providing an overview of all criteria that are fulfilled satisfactorily for the given context and an overview of remaining conflicts. This report is the basis for making the certification decision by the certification body in the certification phase.

The certification phase comprises an assessment of the (report of the) evaluation phase and its results against applicable requirements, that are related to the process of the evaluation phase itself as well as to the security system and the way in which it is operated (i.e. applicable legal requirements and requirements in standards). The certification phase will lead to a certificate that provides assurance that the security system is in accordance with all applicable requirements, including the various stakeholder's perspectives.

Figure 1 shows the two main phases of the methodology, based on the functional approach to conformity assessment in the ISO/IEC 17000- series of standards.

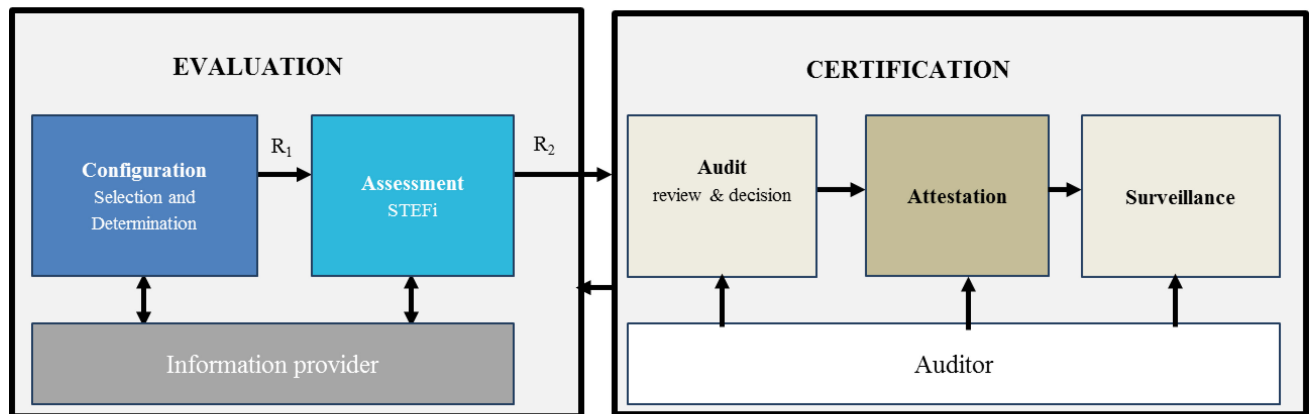


Figure 1 — The two phases of the methodology

Source: Hirschmann, Nathalie, Sophie Wohlgemuth, Leon Hempel, Simone Wurster, Cristina Pauner, Artemi Rallo, Rosario García, Jorge Viguri, Shirin Golyardi, Dick Hortensius, Jelena Burnik, Andrej Tomšič, Thordis Sveinsdottir, Kush Wadhwa, Irene Kamara, Paul De Hert, Roger von Laufenberg, Reinhard Kreissl, “Final Certification Manual”, DEL 6.2, CRISP Project, July 2016, p. 38.

3.2 The four dimensions

3.2.1 Introduction

STEFi stands for Security, Trust, Efficiency, and Freedom infringement and is an evaluation approach that integrates different dimensions in order to ensure that all relevant aspects and stakeholder perspectives are addressed during an assessment process. The four STEFi dimensions have a systematising function, as they allow for structuring the field of a diverse stakeholder community on a first level by assembling related aspects or criteria, notions or concepts as they occur in the field.

This also means that each stakeholder (group) can typically be allocated to at least one of the four dimensions as, for instance, presented in Figure 2.

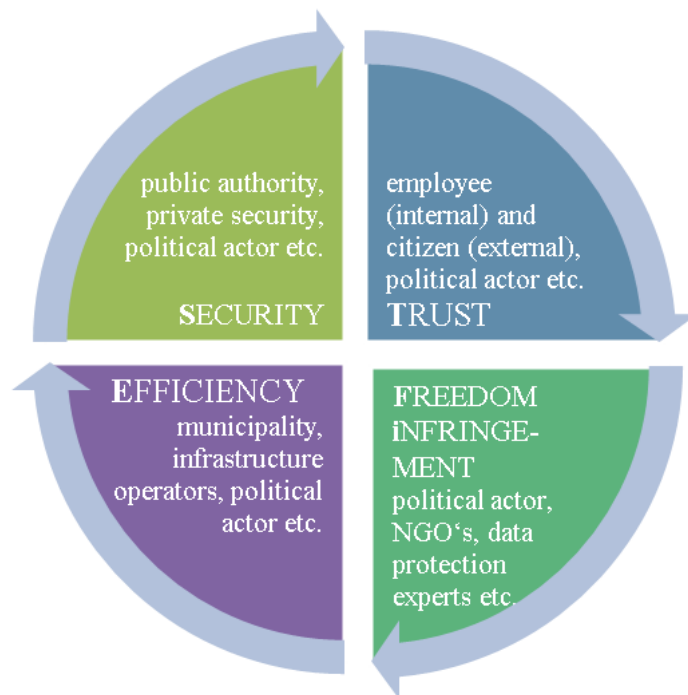


Figure 2 — CRISP's core dimensions and typical stakeholder classification

Source: Hempel, et al., op cit., October 2015, p. 28. According to Hempel, et al., op. cit., 2013; SIAM project.

3.2.2 The Security Dimension

In general terms, security is a concept which has different uses and meanings. It is a highly dynamic concept and adapted to changing conditions such as the societal needs, the needs of citizens, technical options and market practices.

Also in the framework of EU legislation, security has a variety of notions; legal texts use the term in different contexts (terrorism, severe and organized crime, natural disasters, pandemic and major technical accidents). Hence, the meaning of the concept "security" is very much determined by the specific context in which it is used. The definition applicable to this CWA is provided in 2.1.20.

Furthermore, to acknowledge the different aspects of security and to specify the scope to which the evaluation methodology can be applied the following areas are defined⁴:

- **security of citizens** including counter terrorism, prevention of crime and organized crime, and public order, as necessary subareas. In general it covers all possible threats aiming at European citizens, in public and semi-public spaces as well as in private spaces, as a result of an intended/deliberate attack or a natural hazard, by trying to create a peaceful environment, including the prevention of radicalisation;
- **security of infrastructures** includes the security of energy, transportation and telecommunication, supply chains, financing, health infrastructure, and also control systems - general infrastructures which are of high importance of the functioning of a vital society (e.g. clean water supplies and sewerage systems) and thus a protection against threats aiming at the

⁴ Fritz, Florian, et al. op. cit., DEL 1.1 CRISP Project, 15 February 2016, p. 13.

disruption or destruction of these plays an important role in the European policy making and the security industry;

- **border security** includes the means for providing security of land, air and sea border entry points, but also of borders in embassies in order to prevent the illegitimate crossing of people. Further focus on border security aims also at the detection of illegal and dangerous or unsafe products, goods and substances within custom services;
- **crisis management** includes mainly the restoration of security in the aftermath of a crisis, which may result from a natural disaster, but also from deliberate attacks. Furthermore, a focus within the European Union policy lies on the prevention and preparedness of crisis and disaster. This application area is not to be confused with the crisis management in terms of bank recovery, which is currently being discussed on a European level as well.

The security dimension is the most common focus of certification schemes for security systems, i.e. assessment against technical requirements on the proper functioning of security systems and/or the components.

Security addresses both the security of (the operation of) the system as a system and the capabilities of the system to detect and identify individuals, objects, and incidents considered as security threats. In the context of STEFi, the security dimension involves different aspects of security expressed in assessment questions and assessment requirements. It addresses the question of whether the security system is adequate for identifying potential threats to security and whether the functionality of the security system fulfils technical specifications as well promises to and expectations from stakeholders regarding its performance. Amongst others, it addresses risk assessments generally, and more specifically the detection rate and the false alarm rate as well as the impact of intended interference or the level of resilience to potential incidents. It also addresses the definition of relevant forms of behaviour, groups and individuals providing the basis for identification of potential security threats. Lastly, security addresses also the robustness of the system itself against external threats and its operability and resilience in case of possible disruptions.

3.2.3 The Trust Dimension

Trust in a security system is a complex and multi-dimensional matter. It is difficult to achieve and easy to lose. Trust is not a one-time result of a built system design but must be continuously gained during a system's life-cycle. The dimension encompasses the experience with and subjective perception of a security system in regard to its actual performance, by employees, as well as by persons scrutinised by the security system, for example, passengers at an airport. Both experience and the subjective perception determine whether a security system is meeting an appropriate acceptance level. Trust means a firm belief or general confidence that the operation of the security system is reliable and doing its job to preserve security while at the same time respecting personal rights and interests of consumers. Individuals and organisations, consumers, scrutinised and providers all put trust in a security system when it works in a predictable and acceptable manner, has the required quality characteristics for its intended purpose and involves no risk for the operators and scrutinized persons.

In the context of STEFi, the trust dimension reflects a wide range of issues in the assessment questions and requirements, many of which have strong links to other STEFi dimension's requirements; they include availability, usability, reliability, transparency, openness, fairness and accountability, habitus (e.g. in the context of usability), emotions and cognition.

3.2.4 The Efficiency Dimension

Large investments in security technologies actually do have an economic impact on the company, organization, region or state that uses them. The possibility of integration of new technologies with or into existing systems is for example essential from an economic perspective for companies investing in security products and it is therefore considered as a criterion in the STEFi methodology, as well as the

ability to upgrade and update a security system. When taking into account efficiency requirements, such as the throughput in the case of full body scanners, security systems will be compatible with future technological developments and suitable for integration in existing systems. This will promote a continuous investment cycle aimed at updating security technologies and increasing their life-cycle rather than developing complete new systems.

Assessment questions for the efficiency dimension cover all these aspects such as protection measures to avoid misuse or malfunction, as well as general information on product life cycle costs in terms of manpower, operation or deployment and maintenance. Also the quality and quantity of training necessary for the use of a security product are addressed.

3.2.5 The Freedom Infringement Dimension

The Freedom Infringement dimension reflects the impact of a security system on the freedoms and rights of persons. The development of new security technologies is continuously evolving as new security threats appear; many of those have a digital component. Video surveillance systems, for example, not only allow for live monitoring of individuals, but also the recording and retention of images and voices in a recording device or using switched networks, and the use of video analytics or even more sophisticated technologies. Databases and networks are basic elements of current security systems: therefore, one of the main impacts of security systems is enhanced personal data collection, processing, sharing and retention. This affects the (legal) rights to privacy and data protection. Additionally, security systems often affect other rights such as equal treatment and non-discrimination or due process.

The assessment that a security system and its use can have an impact on the freedoms of people is receiving special attention the STEFi approach. For instance, data security is an important element in the Freedom Infringement dimension and requirements related to integrity and confidentiality of recorded data, authorization of access, accuracy and up-to-date assessments or the level of technical and organisational security data measures are considered as part of assessment questions and requirements. Other factors taken into account are whether sufficient defences are put in place in order to protect the privacy and personal data of those scrutinized. The Freedom Infringement criteria also assess whether the intrusiveness of the security system has outweighed the benefits.

Other criteria regarding the operational procedures of the security systems or conditions or the duration of the security measures are related to preventing infringements of the right to due process.

4 Parties involved in the methodology, including their roles and responsibilities

Different parties are involved in the methodology which perform different roles and have different responsibilities.⁵

1. The client⁶: any organization that is applying for certification. The client will in most cases also be the end-user, i.e. the organization that is (planning for) operating a security system. The client shall provide either via the certification body or directly to the evaluation body all documentation and (technical support) information relevant to the system. The client shall permit experts from the evaluation body to access the relevant areas of the site in which the security system operates. The client shall be capable of providing the security system objectives as well as general and specific information on the design (specifications) and operation of the security system, based on a threats analysis related to the objectives of the system. The client will also be involved in responding to assessment questions in those cases where the client has developed the security system and hence has all relevant information about a given system. In case the client cannot provide all relevant

⁵ Hempel, et al., op. cit., October 2015, pp. 50-51.

⁶ According to ISO/IEC 17007:2009: also described as 'first party'.

information, the client shall consult third parties (information provider) during the evaluation phase;⁷

2. The certification body that offers certification according to this methodology. The certification body is therefore in charge of the overall process. They select and contract an independent evaluation body to carry out the evaluation. They decide on basis of a review of the report of the evaluation phase whether the client is eligible for certification;
3. The evaluation body that is contracted by a certification body to conduct an evaluation of an planned or installed security system. The evaluation body shall provide for the project leader and employ or contract experts for the assessment as well information providers. These experts shall be independent from the client and impartial and have sufficient (technical) knowledge of the system to be assessed as well as sufficient expertise on at least one of the STEFi dimensions.

Figure 3 shows the relationship between the evaluation and certification phases and the parties involved. However, the focus of the CWA is on the evaluation phase of the methodology (steps 3, 4 and 5) which is described in more detail in the following clause. Clause 6 briefly refers to the certification phase of the methodology.

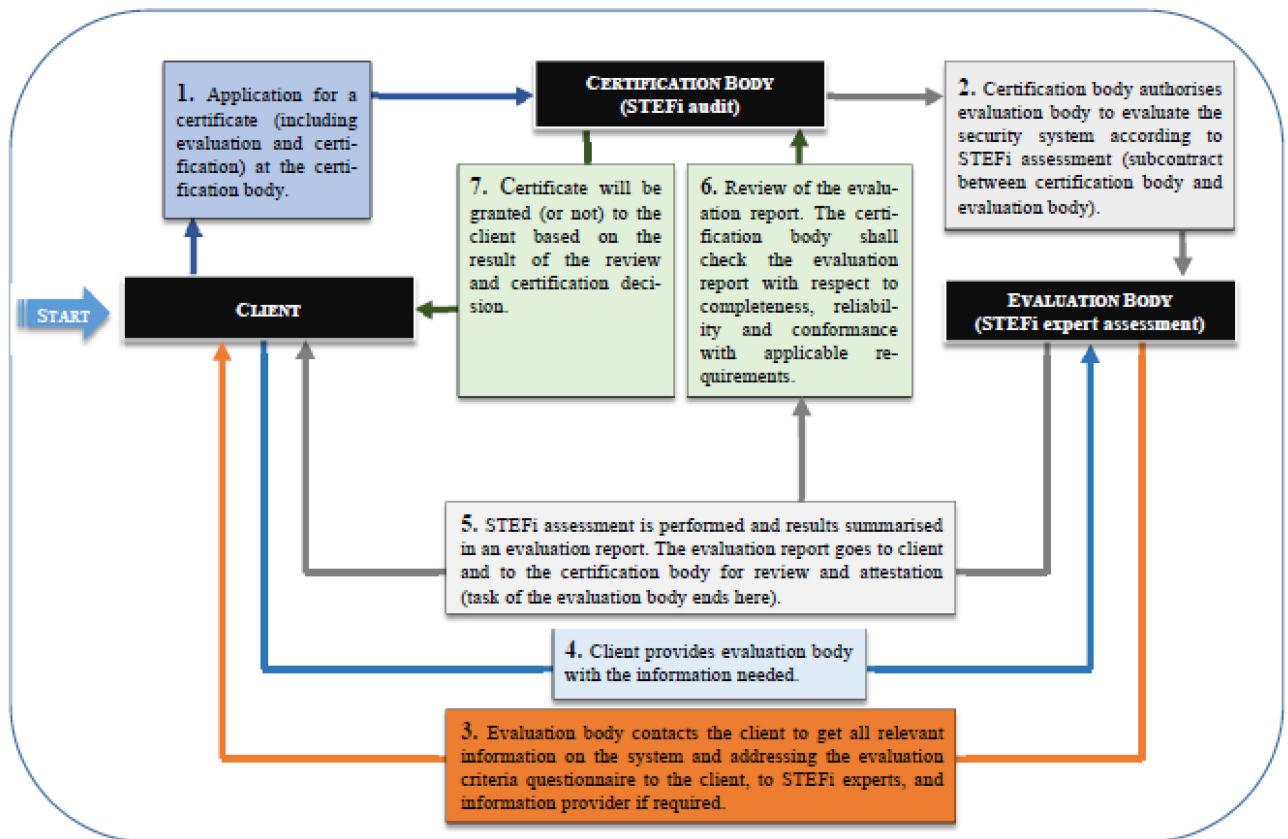


Figure 3 — CRISP evaluation and certification and parties involved - overall picture

⁷ Information provider might be experts either from the clients own company or third parties, who are familiar with the video surveillance system which shall be assessed for being able to proceed in case configuration questions cannot be answered properly Hempel, et al., op. cit., October 2015, p. 45.

Source: Hirschmann, et al., op cit. 2016, p. 23.

5 The evaluation

5.1 Introduction

The following description of the process in the evaluation phase and the involved parties is generally applicable to security systems, but specifically suitable for planned or installed video surveillance systems.

An interested organization (client) needs to apply for certification to a certification body. Once the clients application has been reviewed and accepted, a plan will be established and agreed on. The client shall be capable of providing the security system's objectives as well as ensuring access to general and specific information and data on the operation of the system. The client shall adhere to any conditions set by the certification and evaluation body for guaranteeing a fair, transparent and efficient procedure.

5.2 Roles and responsibilities

Table 1 shows the roles and responsibilities of the stakeholders involved in the evaluation in more detail.

Table 1 — roles and responsibilities during evaluation

stakeholder roles	Responsibility	involved in
project leader	<ul style="list-style-type: none"> - managing the overall evaluation process - setting up (a) new (application) scenario(s) (including general information, technology specifications) - specifying and appointing experts relevant for the evaluation phase, including experts from the client's own organization 	<i>configuration stage & assessment stage</i>
client	<ul style="list-style-type: none"> - providing justification for the need of the security system, e.g. on basis of a risk assessment related to the objectives of the system; - providing access to general and specific information and data on the operation of the system; - answering configuration questions and relevant parts of the assessment questions - providing evidence (such as standards complied with or certificates) when requested - delegating questions to an "information provider" (for verification) if needed - having access to evaluation outputs R_1 and R_2 (both versions) (see 5.4 and Table 3) 	<i>configuration stage & assessment stage</i>
appointed experts	<ul style="list-style-type: none"> - having access to application scenarios (once appointed by the "project leader") - answering the relevant parts of the assessment questions - consulting "information provider" if needed when answering the assessment questions - having access to evaluation outputs R_1 and R_2 (primarily the partial versions) (see 5.4 and Table 3) 	<i>assessment stage</i>
independent "information providers"	<ul style="list-style-type: none"> - answering configuration questions which have been delegated by the client - if applicable, having access to evaluation output R_1 	<i>configuration stage</i>
	<ul style="list-style-type: none"> - answering those questions of the assessment stage which have been delegated by the client and / or by experts - if applicable, having access to evaluation outputs R_1 and R_2 (primarily the partial versions, see Table 3) 	<i>assessment stage</i>

Source: Hempel, et al., op. cit., October 2015, pp. 50-51.

5.3 Competencies of the parties involved

The STEFi approach involves experts to assess a security system from various dimensions. Experts who are selected and appointed by the evaluation body shall have knowledge and experience in one or more of the STEFi dimensions.

NOTE Relevant knowledge and experience will need to be specified in detail in the future certification scheme.

These competencies are most likely covered in general by external stakeholders related to the STEFi dimensions as follows (see also Table 2):

- a) for the evaluation of the security dimension: technical experts (including forensic experts) on security systems;
- b) in relation to the trust dimension: end users (e.g. staff members, consumers, scrutinized) and consumer associations that represent the wider audience. Since the methodology has a European outreach, the involvement of experts of European consumer associations is desirable. In addition, consumer associations operating at national level should be considered for the evaluation, as they represent the local consumer voice, which is an important element;
- c) in relation to the efficiency dimension: specialists for security systems with an economic background and/or relevant technical knowledge (for example, to answer questions on malfunctions, etc.);
- d) in relation to the freedom infringement dimension: human rights experts, data protection lawyers or law professors, because this dimension includes the evaluation of legal and ethical requirements, mainly based on the primary and secondary European law.

Table 2 — Examples of stakeholder groups and possible allocation to STEFi dimensions

Stakeholder group	S	T	E	Fi
Security manager	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Employee/facility personnel	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Facility manager	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Privacy advocate	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Police	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Politician	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Data protection expert	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Manufacturer	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Engineers	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Service provider	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Supplier	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Local authority end-user	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Emergency organisations (end-user)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Operator (end-user)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Law enforcement authority (end-user)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Retail organization (end-user)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Health organization (end-user)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Educational organization (end-user)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
NGO	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Academics (depending on the academic discipline)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Individuals	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Source: Hempel, et al., op cit., October 2015, p. 49. Note: user groups in dependence on CRISP's WP 3 results (Sveinsdottir, Thordis, Rachel Finn, Kush Wadhwa, Rowena Rodrigues, Jolien van Zetten, Simone Wurster, Patrick Murphy, Nathalie Hirschmann, Artemi Rallo, Rosario García, Cristina Pauner, Jorge Viguri, Eva Kalan, Igor Kolar, "Stakeholder Analysis Report", DEL 3.1 CRISP Project, 28. February 2015, pp. 19-34). No exhaustive list.

5.4 Conducting the evaluation

5.4.1 Configuration (selection and determination)

General information on the security system shall be provided by the client in the configuration stage. This includes the following configuration aspects:

- a) specification of the security application area such as 'border security', 'security of the citizens', 'critical infrastructure', 'crisis management', and 'IT-security' (see 3.2.2):
 - spatial information (where is the system located, area covered);
 - time information (operating hours);
 - actors involved in operating the system (operators, scrutinized persons);
 - security function of the security system;
 - primitive functions⁸;
 - connective functions⁹;
 - performative functions¹⁰;
- b) detailed technical specifications of the security system (based on a threats analysis related to the objectives of the system and the context in which it operates):
 - system architecture and integration;

8 "Primitive functions are the basic functions of security PSS [Products, Systems and Services] and are essential for the further performance of other functions. They consist of information collection, storage and management, resulting in databases or other information storages. Locating and tracking can also be classified as a primitive functions, due to the necessity of location and tracking results for the threat assessment, protection of different application areas, or the detention of persons." (Fritz, Florian, et al., op. cit., DEL 1.1 CRISP Project, 15 February 2016, p. 10).

9 "Connective functions make use of the primitive functions, mainly through connecting available information with specific criteria which then again can be necessary for the performance of further security related activities and functions. The most prominent example is the identification function, as it highly depends on (primitive) information collected beforehand, which afterwards is needed if one wants to authorise access. Connective functions are 'verify', 'identify' and 'assess.'" (Fritz, Florian, et al., op. cit., DEL 1.1 CRISP Project, 15 February 2016, p. 10).

10 "Performative functions finally are carried out (security) actions, with a clearly defined and targeted result, making use of one or both of the previous functions. For example in a security related setting, it is not possible to detain a person, if that person has not been identified on basis of available information and has not been located before. Performative functions are 'authorise', 'create situational awareness', 'prevent/protect', 'detain' and 'control.'" (Fritz, Florian, et al., op. cit., DEL 1.1 CRISP Project, 15 February 2016, p. 10).

- technical specifications of all components and the system as a whole;
 - data processing (including data security and protection concepts, if existing);
 - human interaction and co-operation (including any codes of conducts, if existing);
- c) basic information on at least three application scenarios (unless only one or two scenarios apply to the system that is assessed); including:
- scenario framework describing situation, time, space, stakeholders, staff involved and third parties (affected any harmful intervention);
 - risk assessment as basis for establishing the scope of the security system, such as the purpose and objectives, content and context, retention period/duration; consisting of:
 - i. threats analysis to determine the presence of social entities (e.g. intruders, thieves, potential terrorists) within the application scenario that could cause any kind of harmful intervention;
 - ii. vulnerability analysis to determine human and non-human critical points and targets, infrastructures and technologies, including all protection systems, within the application scenario;
 - iii. criticality assessment to determine the magnitude of negative effects if the harmful intervention is successful;
 - a narrative of the security system process from the operator as well the scrutinized person's perspective;
 - scenario extension by indicating best and worst case examples.

Any relevant explanatory information should be documented (amongst others to be accessible in the certification stage).

The scenario descriptions shall be reviewed by the project leader and experts for clarity and completeness and adapted where necessary.

Based on the information collected the project leader shall, in consultation with the client and experts, select all applicable assessment questions from the pool of STEFi assessment questions (see Annex A). If criteria and related assessment questions are missing these shall be added in accordance with the structure of the pool.

NOTE On basis of the results of pilot tests and future practical experiences with the application of the future certification scheme it may be decided that not all assessment questions have the same weight. In that case also the assignment of different weighting factors to the assessment questions will be done by the project leaders based on the information collected during the configuration stage.

The results of configuration stage results are provided in a first output report (R_1), a summary of all the information specified above including the list of applicable STEFi assessment questions. This report functions as input for the assessment stage and as an information source for the experts.

5.4.2 Assessment of the security system using STEFi criteria

The configuration stage is followed by the assessment stage and differs from traditional conformity assessment in various respects. During this stage, the security system is evaluated by using the established assessment questions (derived from the pool of STEFi criteria, see Annex A).

The project leader shall ensure that all questions are addressed and answered by the client and/or the experts (according to their expertise) in order to:

- a) identify any differences in opinions and (expert's) views;
- b) Identify any conflicting criteria for the security system within and between the four dimensions.

The assessment questions incorporate questions with the simple choice of a yes and no answer followed by qualitative answer type questions. This provides more detailed information regarding the security system that is assessed, as well an explanation and justification of any different views between the client and experts.

Each answer shall be accompanied by information providing evidence that can be uploaded (e.g. technical documentation, standards complied with, results of field tests, results of surveys, results of technical evaluations).

If a question cannot be sufficiently answered, the client or expert shall consult an information provider. Any remaining unanswered questions shall be referred to the project leader and included in the final report so that the certification body can decide what the appropriate action should be.

For all assessment questions reference shall be made to appropriate requirements derived from e.g. applicable standards and legislation. These requirements assist in the identification of any conflicts between criteria and to determine the context specific 'acceptability' of the security system and any resolved conflicts as part of the certification phase.

5.4.3 Identification and determination of conflicts

The STEFi evaluation does not only serve the purpose of gathering information on the application of a security system in a specific context, but is also conducted to identify and raise awareness for interrelations and revealing potential conflicts between answers on STEFi questions and related requirements.

Conflicts between criteria are identified on basis of the yes/no answers in three steps.

- 1) Definition of conflict rules between criteria: two criteria are selected and the potential yes/no answers are confronted against each other in a matrix as shown in Figure 4. The "dependent" criterion is on the y-axis, the "independent" criterion on the x-axis. Starting from the perspective of the y-axis it is considered how the answer given on the criterion A conflicts with the answer given on the criterion B on the x-axis. This leads to identification of potential conflicts as indicated in Figure 4. This step shall be repeated for all selected criteria.

		Criterion B ‘Observability’ (T) ‘Are people constantly observed by the system?’	
Criterion A ‘Transparency’ (T) ‘Is the system clear on what it offers?’	RESPONSE OPTIONS	NO	YES
	NO	C⁻ (0)	C⁺ (1)
	YES	C⁻ (0)	C⁻ (0)

C⁻ (0): no conflict;
C⁺ (1): conflict; needs to be addressed.

Figure 4 — Example of a conflict rule matrix

- 2) Identification of actual conflicts: the answers given by the client or experts are put in the matrix established in step 1) and any actual conflicts become evident. No conflicts are scored as ‘0’ and conflicts are scored as ‘1’. This step shall be repeated for all selected criteria.
- 3) Overview of all conflicts: the scores for all sets of selected criteria are transmitted into one overall matrix (see for an example Figure 5). This assists in identifying those criteria that cause most conflicts and therefore also assists in identifying which aspects of the (operation of the) security system need to be addressed with priority to resolve conflicts.

EXAMPLE If criterion A is answered “yes” and criterion B “no” then a conflict might occur between both. For instance, a conflict arises in those cases in which people are constantly observed by a CCTV system, but they are not aware of being scrutinised as no signs indicate the presence of the CCTV system. In the case of an identified conflict, first the additional qualitative answer per criterion and the evidence provided during the assessment stage should be reviewed as this information might assist in clarifying and resolving the conflict. If this is not sufficient, the client will be requested to further review the identified conflict and propose solutions (that may take the form of corrections and corrective actions).


Conflict Matrix		Security			Trust					Efficiency							Freedom				
		Sensitivity	Circumvention	Authentication	Observability	Transparency	Ease	Working environment	Ease	Visibility	Training	Ergonomics	Testing	Trough-put	Maintenance cost	Utility space	Ergonomics	Ergonomics	Non-discrimination	Transparency	Transparency
Security	Sensitivity		1	0	0	0	1	1	1	0	1	1	1	1	0	1	0	0	0	0	1
	Circumvention	1		1	1	1	0	0	0	1	1	0	1	1	0	0	1	1	0	0	1
	Authentication	0	1		1	0	1	1	0	0	1	0	1	0	0	0	1	0	1	0	1
Trust	Observability	0	1	1		1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1
	Transparency	0	1	0	1		1	1	1	1	1	0	0	0	0	0	1	1	1	1	0
	Ease	1	0	1	1	1		1	1	1	1	0	1	0	0	1	1	1	1	1	1
	Working environment	1	0	1	1	1	1		1	1	1	1	1	1	1	1	1	1	1	1	1
	Ease	1	0	0	1	1	1	1		1	1	1	0	0	0	0	1	1	1	1	1
	Visibility	0	1	0	1	1	1	1	1		1	0	0	0	0	0	1	0	1	1	1
Efficiency	Training	1	1	1	0	1	1	1	1	1		1	1	0	0	0	1	1	1	0	1
	Ergonomics	1	0	0	1	0	0	1	1	0	1		0	1	0	0	0	1	1	1	0
	Testing	1	1	1	0	0	1	1	0	0	1	0		1	0	0	1	1	1	1	1
	Trough-put	1	1	0	0	0	0	1	0	0	0	1	1		1	1	1	1	1	0	1
	Maintenance cost	0	0	0	0	0	0	1	0	0	0	0	0	1		0	0	1	0	0	1
	Utility space	1	0	0	0	0	1	1	0	0	0	0	0	1	0		0	1	1	0	1
	Ergonomics	0	1	1	1	1	1	1	1	1	1	0	1	1	0	0		1	1	1	1
	Ergonomics	0	1	0	1	1	1	1	1	0	1	1	1	1	1	1	1		1	1	1
Freedom Infringement	Non-discrimination	0	0	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1		1	1
	Transparency	0	0	0	1	1	1	1	1	1	0	1	1	0	0	0	1	1	1		0
	Transparency	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	1	1	0	
0: no conflict																					
1: conflict																					

Figure 5 — Example of a conflicts summary table

Identified conflicts shall be addressed and resolved by the client in consultation with relevant stakeholders and experts. Conflicts can be resolved by:

- ensuring compliance with applicable legal requirements (where the conflict primarily arises because of non-compliance with legislation);
- implementing technical changes to the security systems and/or changes to the operating procedures that are applied;
- negotiating a solution between different STEFi dimensions by following a practical and legitimate decision-making process, either ending in a majority decision for solving the conflict or in a party taking responsibilities for potential consequences which may address liability issues.

The client shall document the resolving process for each conflict to ensure transparency for all involved parties.

5.4.4 Evaluation report, including conclusions and recommendations

When all the assessment questions in the assessment stage are answered, where applicable with the assistance of consulted information providers and all identified conflicts are addressed adequately, the assessment stage will be closed by the project leader.

The project leader shall prepare an evaluation report (R_2), that includes:

- a summary of how the process was conducted;
- the range of stakeholders involved (e.g. number of experts per STEFi dimension);
- all information gathered during the configuration stage;
- the selected assessment questions (including any weighting factors, see Note to 5.4.1);
- the results of the assessment questions:
 - answers on the yes/no and qualitative answer type questions;
 - the evidence provided to validate the answers;
 - the number of assessment questions that remained unanswered;
- type and number of conflicts that were identified;
- the way in which conflicts have been resolved or the way it is planned to solve them and by when ;
- any remaining unresolved conflicts.

NOTE Interim versions of report R_2 may be provided to the client on a regular basis during the process in the evaluation phase. These reports should provide answers given in the assessment stage including the evidence to validate the answers, as well as a list of questions that have not been answered yet and still need to be taken into account. The reports should also list any deficiencies and/or conflicts already identified as well as solutions already provided by the client. On the one hand, they provide the client with an overview of any remaining actions to take. On the other hand, it assists the evaluation body in monitoring the implementation and the integrity of the STEFi approach. Any observations or irregularities detected in the course of the work should be communicated by the project leader in order to support the evaluation in the most constructive way.

Because the confidentiality of information is a crucial aspect, two different versions of the evaluation report may be prepared, including reduced or extended assessment findings. The characteristics of the contents are given in Table 3.

Table 3 — The characteristics of the two types of evaluation reports R_2

Evaluation Report R_2 [partial]	Evaluation Report R_2 [overall]
Configuration stage output confidential R_1 which includes technical information necessary for the evaluation of a security system.	Configuration stage output confidential R_1 including technical information plus further information, such as uploaded (confidential) information, evidence and stakeholder participation.
Personal contributions per actor role during the assessment stage.	General evaluation (how many assessment questions were answered, not answered, fulfilled, not fulfilled, consultations etcetera to be displayed in percentage).
If applicable, assessment of potential conflicts within the same STEFi criteria.	Listing, description and proposal for addressing potential conflicts within and between STEFi criteria.

Source: Hirschmann, et al., op cit., July 2016, p. 32.

After the views of the client and the experts have been considered and where applicable addressed by the project leader, the evaluation body submits the final evaluation report to the certification body. The confidential evaluation outputs R_1 and R_2 serve as the basis for a third-party review, decision and attestation.¹¹

6 Certification

The purpose of the certification phase is to verify whether the evaluation phase has been conducted according to the applicable requirements (e.g. whether an adequate number and variety of stakeholders with the required competencies has been consulted, whether all relevant configuration and assessment questions have been answered, whether all answered questions have been justified and can therefore be considered to be valid) and whether the requirements related to or derived from the STEFi criteria have been met.

The audit team shall determine whether the evaluation report(s) are complete (information provided, evidences given, conflict solutions provided), reliable and conforms with applicable requirements (to be specified in the future certification scheme). The audit team shall determine the extent to which the requirements related to the STEFi criteria are fulfilled per dimension taking into account the context (situation/scenario) in which the security systems are used. The audit team shall determine whether identified conflicts have been resolved adequately and whether related requirements have been met taking into account the nature of the conflicts and the main purpose of the use of the system and the context in which it is used.

NOTE As part of the future certification scheme rules will need to be developed to determine the acceptable levels of fulfilment of STEFI criteria and conflict resolutions.

The future certification scheme will specify the conditions to determine minor and major conflicts and the possibility for corrective actions. When the client has submitted the required evidence to verify completion of any corrective actions, the certification body will review the corrective action statements and any supplied information for adequacy.

The certificate can only be granted on basis of a positive recommendation of the review of the evaluation stage, including whether identified conflicts have been addressed and resolved adequately and when any necessary corrective action have been completed by the client.

¹¹ Hempel, et al., op. cit., October 2015, p. 48.

Annex A (informative)

STEFi assessment questions and requirements for video surveillance systems

Overview of STEFi dimensions and core questions

Security dimension

1. Are there measures in place for assessing possible threats (prior as well as after the installation of the system) and in further consequence to adequately address situations involving possible threats?
2. Are there measures in place to ensure that the video surveillance system and the operator accurately react to actual security threats?
3. Are there measures in place to ensure that the video surveillance system performs as intended in actual situations of an occurring threat and/or security incident?
4. Does the video surveillance system pose a risk to users/scrutinized and who is accountable for the security actions in relation to the device?

Trust dimension

1. Is the system respectful for users and scrutinized?
2. Is transparency of the system ensured?
3. Is the system reliable for users and scrutinized?
4. Is the system user-friendly?
5. Does the system offer trust tools?

Efficiency dimension

1. Is appropriate information on the system provided?
2. Are appropriate measures implemented to avoid unintended negative economic effects?

3. Does the system allow for appropriate utilization?
4. Is interoperability ensured?
5. Are appropriate lifecycle costs ensured?

Freedom infringement dimension

1. Does the system respect (in terms of installation/design/operation-use) the dignity and customs of the scrutinised?
2. Are due process rights of the individuals affected by the surveillance system guaranteed?
3. Are the basic principles of data protection respected by having measures in place to ensure:
 - that personal data processing is lawful, transparent and fair,
 - that personal data are only processed for a specified purpose,
 - that only the data strictly necessary for a specific purpose are being processed/stored,
 - that personal data processed are accurate,
 - the integrity and confidentiality of personal data being processed,
 - the accountability of the operator of the system.

The list of questions given in in the table is specific for video surveillance systems and not exhaustive and can be adapted depending on the specific system and the context in which it is operated.

Ref.	<u>CRITERION</u> , Attribute	Assessment question	Assessment requirement	Relation with standards or regulation
SECURITY DIMENSION				
S.1	Are there measures in place for assessing possible threats (prior as well as after the installation of the system) and in further consequence to adequately address situations involving possible threats?			
S.1.1	<u>RISK</u> , Threats	<ol style="list-style-type: none"> Has a risk assessment been performed prior to the design and installation of the video surveillance system, assessing the probability and the impact of threats and hazards on the operational site? <i>[yes/no]</i> Which issues have been addressed in the risk assessment and have the results of the assessment been included in the design and installation of the system? <i>[qualitative]</i> 	<p>Prior to video surveillance system design, a risk assessment shall be performed, which will identify threats and hazards to the premises and assess their likelihood.</p> <p>The required security functions for the mitigation of the threats shall be identified and the video surveillance system will be designed in a way to mitigate the assessed risks at the specified location and in regard to the identified threats.</p>	<p>EN-IEC 62676-4 2015 (Clause 4.2ff.)</p> <p>(ISO 31000:2009 describes the principles for the carrying out of a risk assessment.)</p>
S.1.2	<u>RISK</u> , Risk grade and operational requirements	<ol style="list-style-type: none"> Has the video surveillance system been assigned to a security grade? <i>[yes/no]</i> Have specific operational requirements been defined for the video surveillance system and do they explain what it implies for the system to perform as intended? <i>[qualitative]</i> 	<p>The results of the risk assessment shall be used to assign a security grade to the components, sub-systems and functions of the video surveillance system. These shall define the specific operational requirements – the need, justification and purpose – of the system when in operation.</p>	<p>EN-IEC 62676-4 2015 (ibid.)</p> <p>EN-IEC 62676-1-1 Clause 5 (p.28f.) gives more details on the different security grades.</p>
S.1.3	<u>ROBUSTNESS AND SYSTEM INTERFERENCE</u> , Manipulation and Counter-measures	<ol style="list-style-type: none"> Are measures in place, which can prevent the attempt of tampering of the video surveillance system by intruders? <i>[yes/no]</i> How are these measures implemented and do they cover physical as well as virtual/cyber interference attempts? <i>[qualitative]</i> 	<p><i>Camera and system tamper protection/detection</i></p> <p>The camera shall be installed in such a way that it is difficult for an intruder to change the field of view for the camera (e.g. by installing it in a suitable location/height, usage of security fixings, etc.).</p> <p>Also the physical and information system shall be installed in such a way that access and interference to the system (physical and</p>	<p>EN-IEC 62676-4 2015 (p.28.)</p> <p>Grade requirements under BS EN 62676 Clause 9.13. p.25</p> <p>EN-IEC 62676-1-1 Clause 6.3 (p.38f.) gives more details on the System security.</p> <p>EN-IEC 62676-1-2</p>

Ref.	CRITERION, Attribute	Assessment question	Assessment requirement	Relation with standards or regulation
			virtual) is prevented (e.g. by physical and virtual access control systems, assessment of illegal data interference measures). The system shall be inspected in terms of Robustness and interference on a regular basis.	Clause 12 Network Security Requirements <i>COUNCIL FRAMEWORK DECISION 2005/222/JHA, art.3 and art. 4</i> ISO/IEC 27001
S.1.4	<u>ROBUSTNESS AND SYSTEM INTERFERENCE</u> , Detection and Resilience	1. Are there capabilities to recover from an incident? <i>[yes/no]</i> 2. How quickly does the security system recover from an endangering incident and how are such incidents documented? <i>[qualitative]</i>	The video surveillance system shall be able to automatically detect interference and shall issue an alarm in such case. The video surveillance system shall be able to continue operating despite the existence of adverse circumstances (e.g. ability to continue operating during sudden or unexpected loss of power for a significant or defined length of time). The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for the system during an adverse situation.	EN-IEC 62676-4 2015 (p.19.) ISO/IEC 27001:2013 (A.17.1.2) ISO/IEC 27002:2013
S.2	Are there measures in place to ensure that the video surveillance system and the operator accurately react to actual security threats?			
S.2.1	<u>ACCURACY</u> , Sensitivity	1. Are false indicators/incidents by the video surveillance system and/or the operator taken into account? <i>[yes/no]</i> 2. What measures have been taken to prevent a reaction to false indicators/incidents? <i>[qualitative]</i>	The detection and sensitivity of the video surveillance system and its components shall be defined by pass/fail criteria based on resource and risk assessment. The risk assessment shall include defining technical and operational details as defined by the EN-IEC 62676. Where automatic detection, recognition, identification is required, the video motion	EN-IEC 62676-4 2015 EN-IEC 62676-1-1 Clause 6.3.2.3 Tamper protection and detection EN-IEC 62676-1-2 Clause 4.4.6 monitoring of interconnections Home Office Scientific Development Branch CCTV

Ref.	<u>CRITERION</u> , Attribute	Assessment question	Assessment requirement	Relation with standards or regulation
			detector and video content analysis device shall be certified according to its performance requirements for the targeted scenario and environment.	Operational Requirement Manual 2009, Publication No. 28/09 (p.34.). ENIEC CDV 62676-5 Image Quality IEC NWIP 62676-6 VCA Performance Test alias 'CAST iLids Ed2.0' Security Functions, cf. CRISP D1.1
S.2.2	<u>ACCURACY</u> , Deviance and False positives/negatives	<ol style="list-style-type: none"> 1. Are possible false positives and negatives documented? [<i>yes/no</i>] 2. What additional (behavioural) measures are included to prevent a reaction to false indicators/incidents [<i>qualitative</i>] 	<p>Documentation on previously identified false positives/negatives (for example sensor reacts to pets) shall be maintained and shall include specific instructions on how the system as well as the operator can respond to and avoid such events.</p> <p>Where automatic detection, recognition, identification is required, the video motion detector and video content analysis device shall be certified according to its performance requirements for the targeted scenario and environment.</p>	<p>EN-IEC 62676-4 2015 (Clause 5.3; Clause 7; Clause 13).</p> <p>IEC NWIP 62676-6 VCA Performance Test alias 'CAST iLids Ed2.0'</p>
S2.3	<u>ACCURACY</u> , Documentation of false positives/negatives	<ol style="list-style-type: none"> 1. Do the security system produce false positives/negatives? [<i>yes/no</i>] 2. What is the procedure to resolve false positives/negatives? [<i>qualitative</i>] 	<p>Documentation on previously identified false positives/negatives (for example sensor reacts to pets) shall be maintained and shall include specific instructions on how the system as well as the operator can respond to and avoid such events.</p>	<p>EN-IEC 62676-4 2015 (Clause 5.3; Clause 7; Clause 13).</p> <p>IEC NWIP 62676-6 VCA Performance Test alias 'CAST iLids Ed2.0'</p>

Ref.	CRITERION, Attribute	Assessment question	Assessment requirement	Relation with standards or regulation
S.3	Are there measures in place to ensure that the video surveillance system performs as intended in actual situations of an occurring threat and/or security incident?			
S.3.1	<u>PERFORMANCE</u> , Response time/response to incidents	<ol style="list-style-type: none"> 1. Is the response time of the security system kept to an acceptable and specified minimum defined for this site? [yes/no] 2. What is the response time of the security system? [qualitative] 	<p><i>Alarm response</i></p> <p>The signalling indication of an alarm condition to the video surveillance system shall have priority over other security events.</p> <p>It should be defined in the OR whether or not the operator shall be able to take manual control of the system, following an alarm condition, regardless of the degree of automation.</p> <p>Documents pertaining the security staff code of conduct regarding the reporting of incidents, categorization of incidents and their consequent response shall be in place and up-to-date.</p> <p><i>System response times</i></p> <p>System response times shall be kept to an acceptable and specified minimum, as per EN-IEC 62676-4 2015.</p> <p>In order to minimize response times, image capture devices, displays, recording devices, etc. shall be continuously powered and idle, and the system shall not generate more information than the operator can effectively manage.</p>	<p>EN-IEC 62676-4 2015 (p.21)</p> <p>EN IEC 62676-1-1 Clause 6.2.2.3 Events and event driven activities</p> <p>EN IEC 62676-1-2 — Table 4 Video transmission network requirements</p> <p>Art. 38 CFREU, art. 114 and 153 TFEU, art. 3 Directive 2001/95/EC</p> <p>Art. 5 Directive 2001/95/EC</p> <p>ISO 27001</p> <p>Automation of image selection requirements can be found at EN-IEC 62676-4 2015 p.21.</p> <p>Examples of acceptable system response times can be found at EN-IEC 62676-4 2015 p.21.</p> <p>EN IEC 62676-1-1 Clause 8 documentation.</p> <p>EN IEC 62676-1-1 Clause 6.1.3.3 storage</p> <p>EN IEC 62676-1-2 Clause 4.4.4 level of performance</p>

Ref.	<u>CRITERION</u> , Attribute	Assessment question	Assessment requirement	Relation with standards or regulation
S.3.2	<u>PERFORMANCE</u> , Performance as intended	<ol style="list-style-type: none"> Does the documentation of the security system include the likely operating performance or the intended use of the system? <i>[yes/no]</i> How and what is documented? <i>[qualitative]</i> 	<p>The operational requirements (OR) of the video surveillance system shall include:</p> <ul style="list-style-type: none"> the key performance characteristics of the system and its displayed images (e.g. timescale for operator to view persons and track their movements throughout the scene); the degree of image detail required for the observed in each of the live, recorded and exported views (i.e. it may be desirable or appropriate for a different resolution to be used in the live view than in the recorded view); a definition of any image analysis functionality, together with expected accuracy and whether this is to be achieved by the operator or automatically by the system. 	EN-IEC 62676-4 2015
S.3.3	<u>PERFORMANCE</u> , Performance as intended	<ol style="list-style-type: none"> Are there performance review strategies in place? <i>[yes/no]</i> What does the performance review address and how are issues followed up? <i>[qualitative]</i> 	The operator shall periodically assess the intended and actual functionality of the system. These assessments shall be logged and followed up if the actual function doesn't correspond with the intended function documented in the OR.	EN IEC 62676-1-1 Clause 6.3.2.3 Tamper protection and detection. <i>Local legislation:</i> for instance UK Security Industry Act 2001
S.3.4	<u>PERFORMANCE</u> , Performance as intended	<ol style="list-style-type: none"> Are there limits to the detection abilities of the system? <i>[yes/no]</i> What are detection limits? <i>[qualitative]</i> 	<p>The size of an object (target) on the display screen shall have a relation to the required security function, for example identification, recognition, observation, detection or monitoring.</p> <p>The relationship between the camera resolution and the screen display resolution shall be considered; if the camera resolution</p>	EN-IEC 62676-4 2015 (p.24) IEC/CD V 62676-5 Image Quality Performance – camera devices IEC NWIP 62676-6 VCA Performance Test alias 'CAST iLids Ed2.0'

Ref.	<u>CRITERION</u> , Attribute	Assessment question	Assessment requirement	Relation with standards or regulation
			is not equal to the display resolution, the displayed scene may not show the expected amount of detail.	
S.3.5	<u>PERFORMANCE</u> , Performance as intended	1. Are there established mean time period between failures? <i>[yes/no]</i> 2. What is the mean time period between failures? <i>[insert number]</i>	The mean time between failures shall be established based on the components included into the video surveillance system.	IEC 61709:2011
S.4	Does the video surveillance system pose a risk to users/scrutinized and who is accountable for the security actions in relation to the device?			
S.4.1	<u>FAIR DISTRIBUTION OF SECURITY</u> , Safe use	1. Have the operators/users been undergone adequate training on the safe use of the device? <i>[yes/no]</i> 2. How does the training look like to guarantee the safe use of the device? <i>[qualitative]</i>	The OR/ of the video surveillance system shall include specific training information for the operator and shall define the required training for each role involved in the management and operation of the system, including awareness training.	EN-IEC 62676-4 2015 (p.20)
S.4.2	<u>ACCOUNTABILITY AND WITHDRAWAL MECHANISMS</u> , Counter-measures	1. Are there procedures and policies in place addressing issues of accountability of the service provider/product manufacturer? <i>[yes/no]</i> 2. If the video surveillance system shows fails in security, what mechanisms are in place for removal from the site? <i>[qualitative]</i>	Manufacturer's and service provider's guarantees shall be in place and these should include clear instructions on accountability of both parties. Mechanisms for removal of a faulty system shall be in place.	ISO/IEC PDTR CFREU COUNCIL FRAMEWORK DECISION 2005/222/JHA, art.5 Art. 13 Directive 2000/31/EC General Product Safety Directive 2001/95/EC (GPSD). Directive 2011/83/EU on consumer rights
S.4.3	<u>END USER SAFETY</u> , Health and security risk	1. Does the video surveillance system pose any risk to operators (e.g. due to electrical properties or mechanical resistance)? <i>[yes/no]</i>	Risk assessment and health and safety assessment of the video surveillance system shall be carried out periodically.	(art. 3 and 8 Dir. 2001/95/EC) General Product Safety Directive 2001/95/EC

Ref.	<u>CRITERION</u> , Attribute	Assessment question	Assessment requirement	Relation with standards or regulation
		2. How has the risk to persons or infrastructure been assessed (e.g. broken device falling on the ground) and mitigated by appropriate measures? <i>[qualitative]</i>		(GPSD). ISO 45001
TRUST DIMENSION				
T.1	Is the system respectful for users and scrutinized?			
T.1.1	<u>AWARENESS</u> , Training	1. Is the personnel trained to increase awareness of the public on the possible impacts of the system? <i>[yes/no]</i> 2. What kind of training does the personnel receive and how often? <i>[qualitative]</i>	Reference S.4.1 OK The OR/Code of conduct of the video surveillance system shall include specific training information for the personnel to increase awareness of users on the impacts of the exposure to the video surveillance system.	<i>Local legislation:</i> for instance UK Security Industry Act 2001
T.1.2	<u>FEELING OF UNEASINESS</u> , Cultural customs	1. Does the use of the video surveillance system leave a feeling of uneasiness with respect to cultural customs? <i>[yes/no]</i> 2. Under which situation are people compelled to renounce to their cultural customs? (removal of burka, discrimination due to function creep of the video surveillance system) <i>[qualitative]</i>	The design of the scope and capabilities of a video surveillance system shall be developed to minimize its impact on constitutional rights and values, relating to protection of cultural diversity.	Article 21 Charter (to be consistent with Fi2.1)
T.1.3	<u>PHYSIOLOGICAL INVASIVENESS</u> , Health	1. Do users perceive the video surveillance system as a health threat? <i>[yes/no]</i> 2. If yes, is there a (mandatory or voluntary) training or education scheme foreseen to increase awareness of the possible health impacts of the video surveillance system to be deployed? <i>[qualitative]</i>	The video surveillance system shall be deployed in a way that with have no impacts on the health of people (those operating the system and the scrutinized). If the video surveillance system is perceived to have health impacts, there shall be training or educational activities in place to increase awareness.	Code of practice: BSIA Camera Code of Practice

Ref.	CRITERION, Attribute	Assessment question	Assessment requirement	Relation with standards or regulation
T.2	Is transparency of the system ensured?			
T.2.1	<u>TRANSPARENT USE</u> , Up-to-date procedures	1. Is it transparent for users /staff members that the systems is constantly updated/or checked? [<i>yes/no</i>] 2. How is this guaranteed? [<i>qualitative</i>]	Upgrades and technological updates of the video surveillance system shall be reported. Periodic and complete information on the changes shall be released. <i>Reference: E.5.3</i>	Art. 38 CFREU, Art. 169 TFEU, Art. 3 Directive 2001/95/EC
T.2.2	<u>TRANSPARENT USE</u> , Clarity	1. Is the system transparent on the operation, management and performance of the video surveillance system? [<i>yes/no</i>] 2. Specify the procedure, data and people involved to ensure transparency [<i>qualitative</i>]	Transparency of operation, management and performance of the video surveillance system shall be ensured. Any information produced for users shall be provided in clear and understandable terms and under a usable format. <i>Reference: E.1.1</i>	EN IEC 62676-4:2014
T.2.3	<u>TRANSPARENT USE</u> , Complaints	1. Is there a complaint procedure regarding the work of the video surveillance system available to public? [<i>yes/no</i>] 2. Including a detailed description of the complaint procedure (handling, receipting, depositing, reporting)? [<i>qualitative</i>]	An effective procedure for handling concerns and complaints from individuals and organisations about the use of video surveillance systems shall be provided. Information about complaints procedures shall be made readily available to the public.	Code of practice: BSIA Camera Code of Practice No complaint mechanism defined in any technical standard.
T.2.4	<u>TRANSPARENT USE</u> , Performance	1. Does the end user receive clear and concise operating instructions at handover? [<i>yes/no</i>] 2. What is the scope and content of the operating instructions? [<i>qualitative</i>]	At handover, clear and concise operating instructions shall be provided to all system users responsible for operating the system.	Code of practice: BSIA Camera Code of Practice

Ref.	<u>CRITERION</u> , Attribute	Assessment question	Assessment requirement	Relation with standards or regulation
T.3	Is the system reliable for users and scrutinized?			
T.3.1	<u>RELIABILITY</u> , Compliance	1. Does the manufacturer provide a proof of compliance to the operator with product safety legislation? <i>[yes/no]</i> 2. Specify to which legislation the proof refers to. <i>[qualitative]</i>	The video surveillance system manufacturer and the system installer shall provide a proof of compliance with the required product safety legislation, with particular attention to installation in public spaces.	Art. 5 Directive 2001/95/EC EN IEC 62676-4:2014 Clause 16.5 EN 50133-1
T.3.2	<u>MAINTENANCE RESOURCES</u> , Deployment/use/maintenance	1. Is the client supported by a sufficient number of staff for the maintenance of the video surveillance system? <i>[yes/no]</i> 2. According to which technical standards (ISO-EN) are the staff certified? <i>[qualitative]</i>	The operator shall have sufficient and competent technical personnel to maintain and service all its installations in accordance with applicable technical standards including manufacturers' instructions. Reference: T.1.1.	EN IEC 62676-4
T.4	Is the system user-friendly?			
T.4.1	<u>MAINTENANCE</u> , User protection	1. Does the system installer provide information about the installation, commissioning, operation and maintenance of the video surveillance system? <i>[yes/no]</i> 2. How is this information provided? <i>[qualitative]</i>	The system installer shall provide adequate information on installation, commissioning, operation and maintenance of the video surveillance system.	Art. 38 CFREU, Art. 114 and 169 TFEU, Art. 5 Directive 2001/95/EC, Art. 13 Directive 2000/31/EC.
T.4.2	<u>USER ERROR PROTECTION</u> , User protection	1. Does the video surveillance system protect operators against making errors? <i>[yes/no]</i> 2. What are the processes in place to detect errors? <i>[qualitative]</i>	The video surveillance system shall be provided with reliable security measures to mitigate errors and enhance users' protection.	
T.4.3	<u>USABILITY</u> , User protection	1. Can the video surveillance system also be used by less skilled people? <i>[yes/no]</i> 2. How is the system usability ensured? <i>[qualitative]</i>	A usability study shall be conducted in order to assess the effectiveness, efficiency and satisfaction of the video surveillance system for users.	Standards for user-centred system design.

Ref.	CRITERION, Attribute	Assessment question	Assessment requirement	Relation with standards or regulation
T4.4	USABILITY, system integration	1. Are the video surveillance system functions integrated in order to ensure a seamless operation? <i>[yes/no]</i> 2. How is the system integration ensured? <i>[qualitative]</i>	The system installer shall provide appropriate usability testing of the integrated video surveillance system requirements.	Standards for user-centred system design.
T.5	Does the system offer trust tools?			
T.5.1	ENVIRONMENT, User protection	1. Is the video surveillance system respectful with the environment? <i>[yes/no]</i> 2. Which are the solutions provided to avoid an adverse effect on the environment? <i>[qualitative]</i>	The video surveillance system shall be tested/designed to operate in order to prevent any adverse environmental impact.	Art. 114 TFEU EN 50133-1 EN 62676-4 (Clause 5.3.7, Clause 6.4.1; Clause 6.5, Clause 12.9)
T.5.2	ETHICAL CODES, User protection	1. Is there a commitment of the video surveillance system operator to comply with a Code of practice? <i>[yes/no]</i> 2. Report the list of Code of Practices subscribed by the video surveillance operator <i>[qualitative]</i>	The video surveillance system operator shall act within the applicable law and only for the purposes for which it is established or which are subsequently agreed in accordance with a Code of Practice.	Arts. 3 and 5 Directive 2001/95/EC
T.5.3	GOOD PRACTICES/SAFETY CODES, User protection	1. Is there a commitment of the video surveillance system operator to comply with safety codes or good practices? <i>[yes/no]</i> 2. Which are these codes of good practices? <i>[qualitative]</i>	The video surveillance system operator shall comply with the safety codes or good practice in force in the security sector and act in good faith with regard to their basic principles.	Arts. 3 and 5 Directive 2001/95/EC
EFFICIENCY DIMENSION				
E.1	Is appropriate information on the system provided?			
E.1.1	USER MANUAL, Availability	1. Is a user manual provided? <i>[yes/no]</i> 2. What user manual is provided and by whom? <i>[qualitative]</i>	Documentation relating to a video surveillance system shall be concise, complete and unambiguous, including	EN-IEC 62676-1 chap. 8

Ref.	<u>CRITERION</u> , Attribute	Assessment question	Assessment requirement	Relation with standards or regulation
			<p>information to install, put into operation, operate and maintain a video surveillance system.</p> <p>System specification and block diagram incl. specification of configuration shall include the items specified in EN-IEC 62676-1 chap. 8.1.</p> <p>Operational instructions of a video surveillance system shall be designed to minimize the possibility of incorrect operation and be structured to reflect the access level of the user.</p> <p>Information on the minimum required manpower and time shall be given in the user manual.</p> <p>If specific requirements (including on usability) exist for employees who use the security system, they shall be explained appropriately by the vendor of the system.</p> <p>A copy of a user manual shall be provided.</p>	
E.1.2	<u>(SYSTEMS) DOCUMENTATION</u> , Availability	<p>1. Is documentation for the video surveillance system components provided? [yes/no]</p> <p>2. What documentation is provided and by whom? [qualitative]</p> <p>Note Levels of efficiency should be clearly stated, allowing for better comparison with alternatives.</p>	The client shall ensure that the manufacturer provides concise, complete and unambiguous documentation relating to video surveillance system components.	EN-IEC 62676-1 chap. 8
E.2	Are appropriate measures implemented to avoid unintended negative economic effects?			
E.2.1	<u>PROTECTIVE MEASURES</u> TO	1. Are malfunctions and related costs possible? [yes/no]	Instructions relating to the operation of a video surveillance system shall be designed	EN-IEC 62676-1 chap. 8.2, chap. 6.2

Ref.	CRITERION, Attribute	Assessment question	Assessment requirement	Relation with standards or regulation
	<u>ENSURE EFFICIENCY</u> , Possibility of malfunction	2. What malfunctions and related costs are possible and what potential solutions are provided if any? [<i>qualitative</i>]	to minimize the possibility of incorrect operation and be structured to reflect the access level of the user. The system status shall be detected, processed and displayed automatically. Alarm situations shall be identifiable and accessible immediately with a consistent documentation of the event. Evidence of malfunctions and related costs shall be provided.	
E.2.2	<u>PROTECTIVE MEASURES TO ENSURE EFFICIENCY</u> , Possibility of misuse	1. Are misuse and related costs possible? [<i>yes/no</i>] 2. What misuse and related costs are possible and what potential solutions are provided if any? [<i>qualitative</i>]	The video surveillance system shall provide methods for controlled access to data, taking into account the indicated authorization level. Evidence of misuse and related costs shall be provided.	EN-IEC 62676-1, chap. 6.3.2.4.4.
E.2.3	<u>PROTECTIVE MEASURES TO ENSURE EFFICIENCY</u> , Protection measures to avoid other unintended negative economic effects	1. Is there potential for any unintended negative economic effects of an investment in the video surveillance system? [<i>yes/no</i>] 2. What unintended negative economic effects are possible and what potential solutions are suggested if any? [<i>qualitative</i>]	Potential for any unintended negative economic effects of the system shall be documented and solutions shall be suggested. Evidence of potential solutions needs to be provided <i>or an</i> evidence that guarantees, that no unintended negative economic effects are possible.	-
E.3	Does the system allow for appropriate utilization?			
E.3.1	<u>USABILITY</u> , Ergonomics	Based on the system's documentation (e.g. the information in the user manual according to EN-IEC 62676-1):	Operation of the user interface shall be self-explanatory, simple and fast for the operators.	EN-IEC 62676-1

Ref.	<u>CRITERION</u> , Attribute	Assessment question	Assessment requirement	Relation with standards or regulation
		1. Is the video surveillance system user-friendly for the operator? <i>[yes/no]</i> 2. What makes it user-friendly? Please justify your answer. <i>[qualitative]</i>		
E.3.2	<u>USABILITY</u> , Training efforts	1. Are training efforts (including verification) necessary in order to use the system? <i>[yes/no]</i> 2. What training efforts are necessary in order to use the system? <i>[qualitative]</i>	Evidence needs to be provided by checking availability of training verifications/certificates.	
E.3.3	<u>CUSTOMISATION</u> , Documentation	1. Is the extent of possible customisation documented? <i>[yes/no]</i> 2. How and where is customisation documented? <i>[qualitative]</i>	The extent of possible customisation shall be documented and shall be provided as evidence.	
E.3.4	<u>CUSTOMISATION</u> , customer needs	1. Does the video surveillance system allow customisation (to meet the needs of the users)? <i>[yes/no]</i> 2. How are the users given the opportunity to customise the video surveillance system with a range of devices according to their needs? <i>[qualitative]</i>		
E.4	Is interoperability ensured?			
E.4.1	<u>INTEROPERABILITY</u> , Interfaces	1. Are there interfaces to connect the video surveillance system with other systems [as specified in the configuration phase]? <i>[yes/no]</i> 2. Please specify those interfaces and the information they exchange. <i>[qualitative]</i>	If interfaces to other systems exist, they shall be controlled, documented and evaluated in risk assessment.	CLC/TS 50398
E.4.2	<u>INTEROPERABILITY</u> , Documentation	1. If there are interfaces to connect the video surveillance system with other systems, is controlling and documentation of these interfaces	Documentation and controlling process shall be provided as evidence.	

Ref.	CRITERION, Attribute	Assessment question	Assessment requirement	Relation with standards or regulation
		provided? [yes/no] 2. How is controlling and documentation provided/guaranteed? Please explain the controlling and documentation process. [qualitative]		
E.5	Are appropriate lifecycle costs ensured?			
E.5.1	<u>LIFECYCLE COSTS</u> , Maintenance	1. Are maintenance costs calculated? [yes/no] 2. How are maintenance costs calculated? Please specify the calculated maintenance costs [insert in Euros]	The video surveillance system shall allow for efficient maintenance costs.	
E.5.2	<u>LIFECYCLE COSTS</u> , Components	1. Does the security system allow for the use of replaceable components? [yes/no] 2. Which components are replaceable? [qualitative]	The system shall use replaceable components, wherever possible.	
E.5.3	<u>LIFECYCLE COSTS</u> , Technical updates and upgrades	1. Does the system provider allow frequent upgrades, technological updates or other add-ons to the system? [yes/no] 2. What upgrades, technological updates or other add-ons are available in which timeframe? [qualitative]	Upgrades and technological updates shall be allowed whenever available, in particular if the system includes software.	
E.5.4	<u>ENERGY EFFICIENCY</u> , Documentation of consumption	1. Is the energy consumption of the video surveillance system documented? [yes/no] 2. Where and how is the energy consumption documented? [qualitative]	Information on the consumption of energy by the system shall be included in the system documentation.	

Ref.	<u>CRITERION</u> , Attribute	Assessment question	Assessment requirement	Relation with standards or regulation
FREEDOM INFRINGEMENT DIMENSION				
Fi.1	Does the system respect (in terms of installation/design/operation-use) the dignity and customs of the scrutinised?			
Fi.1.1	<u>PROHIBITION OF DISCRIMINATION</u> , Categorization based on protected characteristics	<ol style="list-style-type: none"> Does the video surveillance system categorize the scrutinised based on race, colour, ethnic or social origin, genetic features, religion or belief, membership of a national minority, property, disability, nationality, age or sexual orientation? [yes/no]. Explain the measures taken to prevent this effect [qualitative]. 	The installed video surveillance system (including its operators, installers) shall not distinguish between sex, race, colour, ethnic or social origin, genetic features, religion or belief, membership of a national minority, property, disability, age or sexual orientation (<i>protected characteristics</i>).	Art. 21 Charter Fundamental Rights EU (national legislation)
Fi.1.2	<u>PROHIBITION OF DISCRIMINATION</u> , Direct discrimination	<ol style="list-style-type: none"> Does the video surveillance system treat scrutinised individuals less favourably than other individuals because of a protected characteristic? [yes/no] Explain the measures taken to prevent this effect [qualitative]. 	The video surveillance system shall not treat scrutinised individuals less favourably than other individuals because of a protected characteristic.	Art. 21 Charter Fundamental Rights EU (national legislation)
Fi.1.3	<u>PROHIBITION OF DISCRIMINATION</u> , Harassment	<ol style="list-style-type: none"> Does the video surveillance system (and its operation) have the potential to lead to conduct relating to the protected characteristics, which violates the dignity of the affected individual or/and is intimidating? [yes/no] Explain the measures taken to prevent this effect [qualitative]. 	The operation, use and function of the video surveillance system shall not instigate harassing activity (activity that violates the dignity of the individual and/or is intimidating), by any party within or out of the organization.	Art. 21 Charter Fundamental Rights EU (national legislation)
Fi.1.4	<u>PROHIBITION OF DISCRIMINATION</u> , Disabilities	<ol style="list-style-type: none"> Does the video surveillance system expose disabilities of scrutinised persons? [yes/no] Explain the measures that are in place to avoid the exposure of disabilities? 	<p>Exposure of disabilities of scrutinised persons from the use of the video surveillance system shall be avoided.</p> <p>The measures implemented by the video surveillance system shall protect the</p>	Art. 21 Charter Fundamental Rights EU (national legislation)

Ref.	CRITERION, Attribute	Assessment question	Assessment requirement	Relation with standards or regulation
		[qualitative]	integrity of the person with disability (right to be treated with humanity and dignity).	
Fi.1.5	<u>PROHIBITION OF DISCRIMINATION, Victimization</u>	1. Does the person that complained for discrimination receive adversely treatment? <i>[yes/no]</i> 2. What are the measures to prevent such effect? <i>[qualitative]</i>	A scrutinised individual that complains for discriminatory treatment shall not be adversely treated than other individuals.	Art. 21 Charter Fundamental Rights EU (national legislation)
Fi.1.6	<u>PROHIBITION OF DISCRIMINATION, Training</u>	1. Does the operator provide periodic/regular training and education material to its personnel dealing with the video surveillance system? <i>[yes/no]</i> 2. What kind of training and education is provided, to whom and how often? <i>[qualitative]</i>	The organization shall provide effective training and education of personnel, and implement internal organisational policies to avoid any kind discrimination.	Art. 21 Charter Fundamental Rights EU (national legislation)
Fi.1.7	<u>PROHIBITION OF DISCRIMINATION, Equality Impact assessment</u>	1. Did the operator perform an equality impact assessment? <i>[yes/no]</i> 2. Which were the questions in the impact assessment and what was the result? <i>[qualitative]</i>	The operator shall perform an equality impact assessment before start using the video surveillance system and repeat on an annual basis.	Art. 21 Charter Fundamental Rights EU (national legislation)
Fi.1.8	<u>PROHIBITION OF DISCRIMINATION, Prior consultation with authorities</u>	1. Have the competent authorities on equal treatment and non-discrimination been consulted prior to the use of the video surveillance system? <i>[yes/no]</i> 2. Which authorities have been consulted and how have their recommendations been implemented? <i>[qualitative]</i>	The operator shall consult with competent authorities on equal treatment and non-discrimination, prior to the use of the video surveillance system, in case of compulsory national legislation.	Art. 21 Charter Fundamental Rights EU (national legislation)
Fi.1.9	<u>PROHIBITION OF DISCRIMINATION,</u>	1. Does the video surveillance system impact on fundamental rights of the	The design of the scope and capabilities of a video surveillance system shall be	Art. 21 Charter

Ref.	CRITERION , Attribute	Assessment question	Assessment requirement	Relation with standards or regulation
	Respect for cultural customs	<p>people? <i>[yes/no]</i></p> <p>2. Under which situation are people compelled to renounce their cultural customs? (removal of burka, discrimination due to function creep of the video surveillance system) <i>[qualitative]</i></p>	developed to minimize its impact on fundamental rights and values related to cultural customs.	
Fi.2	Are due process rights of the individuals affected by the surveillance system guaranteed?			
Fi.2.1	<u>DUE</u> _____ <u>PROCESS</u> , Deadlines and processes	<p>1. Does the operator provide processes and reasonable time-framework for the scrutinised to object or appeal against the video surveillance system as a security measure? <i>[yes/no]</i></p> <p>2. Document the processes in place. <i>[qualitative]</i></p>	The operator shall provide processes (such as complaint mechanisms) that guarantee reasonable time framework, so that the scrutinised individuals can decide upon, object or appeal against the security measure.	Art. 47 Charter of Fundamental rights – right to an effective remedy and to a fair trial.
Fi.3	Are the basic principles of data protection respected by having measures in place to ensure: <ul style="list-style-type: none"> • that personal data processing is lawful, transparent and fair, • that personal data are only processed for a specified purpose, • that only the data strictly necessary for a specific purpose are being processed/stored, • that personal data processed are accurate, • the integrity and confidentiality of personal data being processed, • the accountability of the operator of the system. 			
Fi.3.1	<u>PERSONAL</u> _____ <u>DATA</u> , Lawfulness, fairness and transparency	<p>1. Is there adequate legal ground for the operation of the video surveillance system, is the operation of the system done fairly and in a transparent manner in relation to the data subject? <i>[yes/no]</i></p> <p>2. What are the legal provisions and or written elaborations of the legal ground? <i>[qualitative]</i></p>	Personal data shall be processed by the video surveillance system lawfully, fairly and in a transparent manner in relation to the data subject,	Art 5.1a, 6, 7, 8, 9 GDPR, Provisions in national legislation (if existing).

Ref.	CRITERION , Attribute	Assessment question	Assessment requirement	Relation with standards or regulation
Fi.3.2	<u>PERSONAL DATA</u> , Information to data subject	<ol style="list-style-type: none"> 1. Is the operation of the video surveillance system transparent to the individuals, are they adequately informed about it? <i>[yes/no]</i> 2. Where are the notices displayed, are they visible, readable and comprehensive? <i>[qualitative]</i> 	Operator of the video surveillance system (data controller) shall provide data subject with relevant information on processing of personal data in line with conditions from GDPR Articles 12–14.	Art. 12–14 GDPR
Fi.3.3	<u>PERSONAL DATA</u> , Consent as legal ground for processing	<ol style="list-style-type: none"> 1. If consent is required for processing of personal data for a particular use case of the video surveillance system, does the consent meet the requirements for consent from GDPR Article 7 and 8? <i>[yes/no]</i> 2. What evidence does the controller maintain to demonstrate acquired consent? <i>[qualitative]</i> 	Operator of the video surveillance system (data controller) shall meet the conditions for consent from GDPR Article 7 and 8.	Art 7, 8 GDPR
Fi.3.4	<u>PERSONAL DATA</u> , Processing of special categories of personal data	<ol style="list-style-type: none"> 1. If special categories of data are extracted from video images and are further processed, are the conditions for processing of sensitive data from the GDPR Article 9 met? <i>[yes/no]</i> 2. Which safeguards for protection of sensitive data are employed? <i>[qualitative]</i> 	Processing of special categories of personal data by the video surveillance system shall be in line with conditions from GDPR Article 9.	Art. 9 GDPR
Fi.3.5	<u>PERSONAL DATA</u> , Automated individual decision-making, including profiling	<ol style="list-style-type: none"> 1. Is the individual subjected to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her? <i>[yes/no]</i> 2. What is the basis for such data 	Automated individual decision-making, including profiling done by the video surveillance system shall be in line with conditions from GDPR Article 22.	Art 22 GDPR

Ref.	<u>CRITERION</u> , Attribute	Assessment question	Assessment requirement	Relation with standards or regulation
		processing (from Article 22(2) and what measures are in place to safeguard the rights and interests of the individuals concerned? <i>[qualitative]</i>		
Fi.3.6	<u>PERSONAL DATA</u> , Joint controllers	<ol style="list-style-type: none"> Are more legal persons involved in the processing and/or use of the video surveillance system? <i>[yes/no]</i> How are the roles defined and shared among such controllers? <i>[qualitative]</i> 	Where two or more controllers jointly determine the purposes and means of processing, the processing shall be in line with conditions from GDPR Article 26.	Art 26 GDPR
Fi.3.7	<u>PERSONAL DATA</u> , Processors	<ol style="list-style-type: none"> If processing (or any part of) of video surveillance is outsourced to a processor or sub-processor is the processing in line with conditions from GDPR Articles 28 and 29? <i>[yes/no]</i> Which are the guarantees provided by the processor or sub-processor which operate on behalf of the controller? <i>[qualitative]</i> 	Where processing by the video surveillance system is carried out on behalf of a controller, the processing shall be in line with conditions from GDPR Articles 28 and 29.	Art 28 and 29 GDPR
Fi.3.8	<u>PERSONAL DATA</u> , Transfers of personal data to third countries or international organisations	<ol style="list-style-type: none"> If video material or the personal data extracted from it is transferred to third countries are these transfers in line with conditions from GDPR Articles 44–49? <i>[yes/no]</i> What is the basis of such transfer (provide documentation, DPA decisions, contractual clauses, etc.) and which procedures are in place to monitor lawful transfer of personal data? <i>[qualitative]</i> 	Transfers of personal data processed by video surveillance system to third countries or international organisations shall be in line with conditions from GDPR Articles 44–49.	Art 44–49 GDPR
Fi.3.9	<u>PERSONAL DATA</u> , Data subjects rights and restrictions	<ol style="list-style-type: none"> Does the operator have the necessary policies and procedures in place in order to execute individual's requests in 	Operator of the video surveillance system (data controller) shall be able to execute data subject's rights in line with conditions	GDPR: • Art 15

Ref.	CRITERION, Attribute	Assessment question	Assessment requirement	Relation with standards or regulation
	<ul style="list-style-type: none"> • to access • to rectify • to erasure ('right to be forgotten') • to restriction of processing • to data portability • to object 	<p>due time and scope whilst respecting possible restrictions of individual's rights? <i>[yes/no]</i></p> <p>2. Which procedures are in place to ensure timely and adequate execution of data subjects rights? <i>[qualitative]</i></p>	from GDPR Articles 15–21. Restrictions of data subject rights, provided by Union or member State by way of a legislative measure, shall be respected	<ul style="list-style-type: none"> • Art 16 • Art 17 • Art 18 • Art 20 • Art 21 • Art. 23
Fi.3.1 0	<u>PERSONAL DATA</u> , Purpose limitation	<p>1. Are the purposes of processing of video footage clearly defined and limited? <i>[yes/no]</i></p> <p>2. How is the purpose limitation principle implemented in practice (provide evidence of documentation, internal policy, etc.)? <i>[qualitative]</i></p>	The video surveillance system shall collect personal data for specified, explicit and legitimate purposes and these shall not be further processed in a manner that is incompatible with those purposes.	Art 5.1b GDPR Provisions in national legislation (if existing).
Fi.3.1 1	<u>PERSONAL DATA</u> , Data minimization	<p>1. Is the scope of surveyed area minimized in relation to the purposes? Are technical and/or organisational measures in place in order to limit the scope and duration of surveillance? <i>[yes/no]</i></p> <p>2. Is there a documented data protection impact assessment covering data minimization principle? <i>[qualitative]</i></p>	Personal data processed by the video surveillance system shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.	Art 5.1c GDPR Provisions in national legislation (if existing).
Fi.3.1 2	<u>PERSONAL DATA</u> , Storage limitation	<p>1. Is the retention limit of video footage and/or the personal data potentially extracted form it clearly defined? Does the retention time reflect the minimum time that is necessary for the purposes for which the personal data are processed? <i>[yes/no]</i></p>	Personal data processed by the video surveillance system shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.	Art 5.1e GDPR Provisions in national legislation (if existing).

Ref.	<u>CRITERION</u> , Attribute	Assessment question	Assessment requirement	Relation with standards or regulation
		2. How are retention limits enforced in practice? <i>[qualitative]</i>		
Fi.3.1 3	<u>PERSONAL DATA</u> , Processing which does not require identification	1. If the purposes for which the operator processes personal data do not or do no longer require the identification of a data subject by the controller, does the controller maintain, acquire or process additional information in order to identify the data subject? <i>[yes/no]</i> 2. What are the internal policy provisions to ensure non identification? <i>[qualitative]</i>	Processing personal data by video surveillance system which does not require identification shall be in line with conditions from GDPR Article 11.	Art. 11 GDPR
Fi.3.1 4	<u>PERSONAL DATA</u> , Data accuracy	1. If video surveillance system processes other data than video images, what are the false positive/negative rates and are procedures to deal with them clearly defined? <i>[yes/no]</i> 2. Which procedures are in place to ensure data accuracy? <i>[qualitative]</i>	Personal data processed by the video surveillance system shall be accurate and, where necessary, kept up to date.	Art 5.1d GDPR Provisions in national legislation (if existing).
Fi.3.1 5	<u>PERSONAL DATA</u> , Integrity and confidentiality	1. Are technical and organisational measures and procedures for data security (such as user rights management, physical security, access logging, secure disposal of data and data media, etc.) in place and regularly reviewed? <i>[yes/no]</i> 2. Which technical and organization measures and procedures are in place to provide adequate data security, how is the process of continuous improvement implemented? <i>[qualitative]</i>	The video surveillance system operator and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons,	Art 32 GDPR ISO/IEC 27001:2013 ISO/IEC 27002:2013 EN IEC 62676-1-1- Clause 6.3.3, Image and data integrity

Ref.	CRITERION, Attribute	Assessment question	Assessment requirement	Relation with standards or regulation
Fi.3.1 6	<u>PERSONAL DATA</u> , Notification of a personal data breach	<ol style="list-style-type: none"> 1. Are procedures, data and human/technical resources place in order to ensure that personal data breach notification duties are carried out in due time and scope? <i>[yes/no]</i> 2. Does breach notification policy cover roles and responsibilities, procedures, timeframes, necessary data and channels for notification? <i>[qualitative]</i> 	The video surveillance system operator shall have the procedures, data and human and technical resources in place to fulfil its personal data breach notification duties to the supervisory authority and/or to the data subject, in compliance with conditions from GDPR Articles 33–34.	Art 33, 34 GDPR
Fi.3.1 7	<u>PERSONAL DATA</u> , Accountability	<ol style="list-style-type: none"> 1. Is the performance of the video surveillance system regulated by internal policy of the operator? Are the provisions of such internal policy in line with GDPR and relevant national legislation? <i>[yes/no]</i> 2. Which processes, data and people are in place to enforce accountability? <i>[qualitative]</i> 	The video surveillance system operator shall be responsible for, and able to demonstrate compliance with principles relating to processing of personal data.	Art 5.2 GDPR Provisions in national legislation (if existing).
Fi.3.1 8	<u>PERSONAL DATA</u> , Data protection by design and by default	<ol style="list-style-type: none"> 1. Does the operator take into account the principles of data protection by design and by default from design phase throughout the lifecycle of operation of video surveillance system? <i>[yes/no]</i> 2. Which procedures, data and people are involved in assurance of data protection by design and by default? <i>[qualitative]</i> 	The video surveillance system operator shall respect the principles of data protection by design and by default in line with conditions from GDPR Article 25.	Art 25 GDPR
Fi.3.1 9	<u>PERSONAL DATA</u> , Data protection impact assessment	<ol style="list-style-type: none"> 1. Did the operator carry out an impact assessment (DPIA) of the envisaged processing operations of video surveillance system on the protection of personal data in line with conditions 	The video surveillance system operator shall carry out an impact assessment of the envisaged processing operations on the protection of personal data in line with conditions from GDPR Article 35.	Art 35 GDPR

Ref.	<u>CRITERION</u> , Attribute	Assessment question	Assessment requirement	Relation with standards or regulation
		from GDPR Article 35? <i>[yes/no]</i> 2. What does the DPIA cover? <i>[qualitative]</i>		
Fi.3.2 0	<u>PERSONAL DATA</u> , Prior consultation	1. Did the operator of the video surveillance system consult the supervisory authority prior to processing in line with requirements from GDPR Article 36? <i>[yes/no]</i> 2. What documentation is provided by the operator (especially concerning the remaining risks that could not be mitigated, based on the results of the DPIA) and what is the outcome of the consultation? <i>[qualitative]</i>	The video surveillance system operator shall consult the supervisory authority prior to processing in line with conditions from GDPR Article 36.	Art 36 GDPR
Fi.3.2 1	<u>PERSONAL DATA</u> , Data protection officer	1. If nomination of a data protection officer is necessary, has such officer been nominated in line with GDPR requirement and does he or she perform their duties foreseen by GDPR? <i>[yes/no]</i> 2. Which resources (in terms of staff, skills and budget) and other preconditions are in place for DPO to successfully fulfil its tasks? <i>[qualitative]</i>	The video surveillance system operator and the processor shall fulfil their duties as data protection officer in line with conditions from GDPR Articles 37–39.	Art 37–39 GDPR
Fi.3.2 2	<u>PERSONAL DATA</u> , Codes of conduct	1. If the operator signed a code of conduct regulating aspects of video surveillance systems pertaining to processing of personal data, does it adhere to requirements of such code of conduct? <i>[yes/no]</i> 2. Which principles are covered by the code, what is the procedure for supervision of the code and how is	The video surveillance system operator shall comply with codes of conduct in line with conditions from GDPR Articles 40–41 .	Art 40–41 GDPR (Adherence to codes of conduct under GDPR is voluntary).

Ref.	<u>CRITERION</u> , Attribute	Assessment question	Assessment requirement	Relation with standards or regulation
		enforcement of the code ensured?? [qualitative]		
Fi.3.2 3	<u>PERSONAL DATA</u> , Certification	<ol style="list-style-type: none"> Has the operator obtained a certificate under the conditions prescribed by GDPR Articles 42 and 43? [yes/no] Who issued the certificate and what is the scope of the obtained certification (provide all relevant documentation)? [qualitative] 	The video surveillance system operator or data processor shall provide proof of certification in line with conditions from GDPR Articles 42–43.	Art 42–43 GDPR (Certification under GDPR is voluntary).
Fi.3.2 4	<u>PERSONAL DATA</u> <u>Training</u>	<ol style="list-style-type: none"> If the operator is obliged to provide appropriate periodic training for the personnel having permanent or regular access to personal data, is such training in place? [Yes/no] What are the content and procedure of such training? [qualitative] 	The video surveillance system operator shall conduct appropriate periodic training for the personnel having permanent or regular access to personal data if obliged to do so by GDPR Articles 39 and 47, or other legal requirements.	Article 39, article 47, other legal requirements (national).

Annex B (informative)

Standards specifying requirements for the evaluation process

NOTE As the standardization landscape is dynamic, standards series instead of single standards are presented in the overview below. The system-related standards refer to video surveillance systems, which were chosen as CRISP's first application area.

Relevant standards and regulations for evaluation and certification

- ISO/IEC 17000- series Conformity assessment, in particular ISO/IEC 17065 Conformity assessment – Requirements for bodies certifying products, processes and services¹² and ISO/IEC 17020 Conformity assessment – Requirements for the operation of various types of bodies performing inspection.
- Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)

Relevant standards for technical aspects of the systems

- EN 50130 series Alarm systems¹³
- EN-IEC 62676 series Video surveillance systems for use in security applications
- IEC 61709 Electric components – Reliability
- ISO 31000 Risk management – Principles and guidelines
- ISO 45001 Occupational health and safety management systems – Requirements with guidance for use
- CLC/TS 50398 Alarm systems - Combined and integrated alarm systems - General requirements

Relevant standards and regulations for the freedom infringement/legal perspective

- ISO/IEC 27000- series Information technology – Security techniques – Information security management systems¹⁴

¹² See website of ISO/IEC's relevant committee SO/CASCO Committee on conformity assessment: ISO, "Standards catalogue. ISO/CASCO – Committee on conformity assessment", no date. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=54998&published=on&includesc=true and ISO, "Resources for conformity assessment – The CASCO Toolbox", no date. http://www.iso.org/iso/home/about/conformity-assessment/conformity-assessment_resources.htm.

¹³ See website of CENELEC's relevant committee CLC/TC 79 Alarm systems: CENELEC, "Standards Development – Technical Bodies", 2016. https://www.cenelec.eu/dyn/www/f?p=104:7:0:::FSP_ORG_ID:73.

- ISO/IEC 29000- series Information technology – Security techniques¹⁵
- EU Charter of Fundamental Rights¹⁶ (Arts. 7, 8, 21, 24, 25, 45, 47, 48, 49)
- European Convention of Human Rights¹⁷ (Arts. 6, 7, 8, 13, 14)
- General Data Protection Regulation (GDPR) 679/2016
- General Product Safety Directive (GPSD) 2001/95/EC
- Directive on electronic commerce, 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce
- Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems
- Consolidated version of the Treaty on the Functioning of the European Union

14 See website of ISO/IEC's relevant committee ISO/IEC JTC 1/SC 27 - IT Security techniques: ISO, "Standards catalogue. ISO/IEC JTC 1/SC 27 - IT Security techniques, no date. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=45306.

15 See website of ISO/IEC's relevant committee ISO/IEC JTC 1/SC 27 - IT Security techniques: ISO, "Standards catalogue. ISO/IEC JTC 1/SC 27 - IT Security techniques, no date. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=45306.

16 Official Journal of the European Union, Charter of Fundamental Rights of the European Union, 2012/C 326/02, <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN>.

17 European Court of Human Rights, Council of Europe, European Convention on Human Rights, amended by the provisions of Protocol No. 14 (CETS no. 194), https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/Convention_ENG.pdf.