THE SAPIENT CONSORTIUM

SURVEILLANCE IMPACT ASSESSMENT MANUAL

DAVID WRIGHT, INGA KROENER, MONICA LAGAZIO, MICHAEL FRIEDEWALD, DARA HALLINAN, MARC LANGHEINRICH, RAPHAËL GELLERT, AND SERGE GUTWIRTH

This document was developed within the SAPIENT (Supporting fundamentAl rights, PrIvacy and Ethics in surveillaNce Technologies) project by a consortium, consisting of the following partners: Fraunhofer Institute for Systems and Innovation Research (co-ordinator), Trilateral Research & Consulting LLP, Vrije Universiteit Brussel, Università della Svizzera italiana, King's College London, and Centre for European Policy Studies.

The SAPIENT project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement Nº 261698.

E-mail: feedback@sapientproject.eu
Website: http://www.sapientproject.eu

Funded by
the European Union

First edition, April 2015

Contents

List of Figures

1
Preface

This manual consists of two parts. The first part contains the comprehensive SIA methodology produced developed by the SAPIENT consortium. The second contains a revised guide for a small-scale SIA based on the lessons learned during in a number of tests to apply the SIA guidelines. The annex to this deliverable contains the questions for the comprehensive SIA guide, as well as the small-scale SIA guide.

The SAPIENT consortium initially developed a guide for conducting an full SIA based on the principles of risk assessment (Part I of this manual). The guide described a method for identifying, assessing (or evaluating) and prioritising for treatment risks arising from the development and deployment of surveillance technologies, systems and applications. A number of test case studies were undertaken in order to evaluate the SIA guide as a tool for the assessment of new surveillance systems and technologies, for use by organisations. The objective was to test this methodology and revise it in light of feedback and the experience of implementing this methodology in a range of settings and with a number of case studies.

The main result of the tests was that the full SIA process is not suitable for small companies or research projects. Consequently the SAPIENT developed a 10-page guide for a small-scale SIA to be used by this range of organisations (Part II of this manual).

Part I

Guide for a comprehensive Surveillance Impact Assessment

2
Introduction

This guide describes a method for identifying, assessing (or evaluating) and prioritising for treatment risks arising from the development and deployment of surveillance technologies, systems and applications. The SAPIENT consortium has prepared this guide for the developers, operators and regulators of surveillance systems. The method here is somewhat like and is based on a privacy impact assessment (PIA), but with one especially important difference, and that is that a surveillance system or application can have impacts on more than just privacy. It can also have impacts on other fundamental rights. The development and deployment of surveillance systems may have various consequences – societal, economic, political; they may raise legal and ethical issues too.

Ideally, a surveillance impact assessment should be conducted at an early stage, when it is still possible to influence the decision-making process, as to whether a surveillance system is actually warranted and, if so, how it should be configured to avoid being unduly intrusive and what safeguards should be put in place to ensure that it does not infringe upon democratic aspirations. However, the surveillance impact assessment can also be conducted even after a decision has been taken to proceed with the development and deployment of a system as well as after, to ensure the SIA recommendations are implemented.

In the case of a future system, the first question to ask is: "Is such a system needed?" before the question: "Does the (proposed) system merit the conduct of an SIA?". If the project manager cannot answer the first question, the need for an SIA becomes automatic and a logical action. By the same token, in practical terms, it makes sense for an organisation to apply the same assessment process to the risks which might require surveillance and the risks posed by surveillance.

This guide is divided into two main parts, the first of which provides an overview of a risk assessment approach to surveillance, while the second part describes how to conduct a surveillance impact

assessment. In addition, the guide has three annexes, which will help in the conduct of the SIA.

3
Overview of a risk assessment approach to SIA

3.1 Purpose

A surveillance system can raise risks for individuals, groups and organisations, as well as society as a whole.

The purpose of a surveillance impact assessment (SIA) is to assess the risks a surveillance-related project, policy, programme, service, product or other initiative poses for privacy, as well as for other human rights and ethical values. The risk assessment addresses the *likelihood* of a certain event and its *consequences*, i.e., impacts. An SIA should include stakeholder consultation and, ultimately, lead to mitigating measures as necessary in order to avoid, minimise, transfer or share the risks. The SIA should follow a surveillance initiative throughout its life cycle. The project should revisit the SIA as it undergoes changes or as new risks arise and become apparent.

While privacy and data protection impacts are a major focus of an SIA, surveillance affects a range of other fundamental rights and ethical and social principles that may also be relevant in a particular assessment. The SIA method described in this guide subsumes a privacy impact assessment, i.e., there is nothing in a PIA which is not also included here. In other words, an SIA and a PIA do not need to be conducted as separate exercises. Similarly, the SIA subsumes an ethical impact assessment. Hence, an SIA includes, but is more encompassing than either a PIA or EIA.[1]

A surveillance impact assessment should be undertaken

1. by those developing surveillance systems, technologies or applications and/or
2. by those who are commissioning (procuring) and intending to operate a surveillance system and/or
3. by regulators who want to assess surveillance system proposals.

[1] Two of the authors of this guide have already proposed an integrated privacy and ethical impact assessment. See Wright, David and Michael Friedewald, "Integrating privacy and ethical impact assessment", *Science and Public Policy*, Vol. 40, No. 6, 2013, pp. 755-766.

Surveillance systems can have positive as well negative impacts.[2] This guide reflects the positive impacts, but focuses primarily on the potential negative impacts. An SIA can be used to identify and evaluate these impacts and appropriate mitigation measures. Accordingly, it will be beneficial to sponsors and the public alike for an SIA to be undertaken at as early a stage in the life-cycle of a project as practicable, when it is still possible to influence the design of the surveillance system or to determine whether the system is actually necessary.

[2] For example, many people support the use of CCTV cameras on public transport while those same people may oppose their being tracked across the Internet so that they can be better targeted for personalised advertising.

General principles for the control of surveillance

Four fundamental principles should govern the development and deployment of surveillance systems that may have substantial negative privacy or other implications:

1. Surveillance systems must comply with the law.
2. The prospective developer or operator of a surveillance system should be able to justify the need for the surveillance system. Not only should surveillance be used only when there are no more cost-effective[3] alternatives, but the justification of a surveillance system should be an explanation based on evidence and systemic reasoning, and not merely on assertions. The justification should make clear what less privacy-invasive alternatives have been considered, and why they are inadequate.
3. Surveillance systems must be ethically defensible.
4. The proponent of a surveillance system should be able to demonstrate that the benefits outweigh the negative impact. For example, visual surveillance must be no more intensive (e.g., the number of cameras), and no more extensive (e.g., across a large area) than the analysis justifies.

[3] Cost here should be understood in a wider sense than just monetary cost, for example, social costs, opportunity costs, political costs, etc.

To ensure these principles are applied, three main tasks need to be undertaken preferably be-fore, at the latest during development and, in the worst case, during deployment, of a surveil-lance system:

- The proposed surveillance system must undergo an SIA before or concurrently with development of the technology or system, the purpose of which is to identify and evaluate the risks and to ensure the proposed system does not contravene the public interest. The SIA should involve consultation with stakeholders and be characterised by transparency. The SIA should recommend measures for mitigating the risks identified.
- Mass surveillance systems must be subject to parliamentary or regulatory approval before deployment – i.e., an appropriate organ

of the parliament or a regulator would need to approve a surveillance system before it is deployed. Even after the surveillance system is deployed, it should be subject to controls to ensure that safeguards have been properly implemented and that any breaches are reported promptly and are prosecutable.

- The SIA and the surveillance system should be subject to audit by an independent third party to ensure the SIA recommendations are adopted or, if some are not adopted, that there is adequate justification for why they have not been adopted. A single audit may be inadequate. Audits should be undertaken periodically and when warranted.

3.2 *An overview of risk assessment*

An assessment of the risks or impacts of a proposed surveillance system should

1. identify the risk criteria – the framework within which risks will be assessed
2. identify the risks, which is the process of enumerating feared events from stakeholders and the corresponding threats that might lead to them.
3. analyse the risks, which is the process of understanding the nature of the risk and determining the consequences and likelihood of each risk
4. assess (evaluate) the risks, which is the process of ranking or prioritising the risks: which risks are the most serious and should be dealt with first.

The organisation (the sponsor) that is responsible for the prospective surveillance system should carry out the risk treatment and identify and implement controls or counter-measures to avert the risks. Risk apportionment is an output and even an eventual outcome of an SIA, rather than a controllable variable or something known at the beginning. Risk seldom all falls on one organisation[4] – not even on a sponsor that is criminally negligent. "Responsible" is too easily misunderstood to mean only "legally liable". A sponsor may be legally compliant, but "morally liable".

The assessor should identify, analyse and evaluate the threats and vulnerabilities to individuals and groups (including society), measure the impacts (consequences) of the risk involved, and recommend measures and controls (or safeguards) to manage them.

In general, a risk can be related to or characterised by:

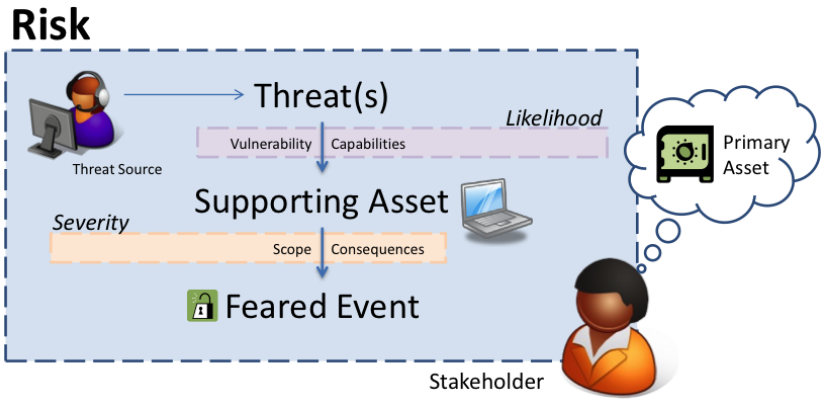
[4] For example, the Snowden revelations have shown that the NSA has been responsible for weakening some crypto systems and their implementations. Arguably, the NSA should have done a risk analysis and, even if it had, the organisations using the crypto systems are now responsible for the risk handling at their sites, even if they didn't cause (or couldn't foresee) the related risks.

1. its origin or domain (i.e., assets and principals involved, time and place of occurrence),
2. a specific activity, event or incident (i.e., feared event),
3. a specific reason for its occurrence (i.e., a threat exploiting a vulnerability),
4. its consequences (i.e., impact). A risk may have monetary, technical, operational and/or human consequences,
5. counter-measures and controls and their effectiveness (or lack thereof).

Figure 3.1 below illustrates the main terms: A *threat source* has certain *capabilities* to exploit *vulnerabilities* in one or more *supporting assets*. If the *threat* exploit[5] the vulnerabilities, it will have certain *consequences* to a *stakeholder's primary asset*s, the *severity* of which is also determined by the *scope* of the *feared event* (i.e., the number of people to which it applies). We call the combination of "threats to supporting assets which bring about a feared event to a stakeholder's primary asset" a *risk*.

[5] We have used the term "exploits" which suggests intention, while recognising that such intention is absent in natural threats, e.g., lightening may threaten a power station. It could "exploit" (without intention) or damage an inadequate infrastructure.

Figure 3.1: Simplified illustration of the risk terminology



We can define the main terms used in the process of risk assessment as follows:[6]

[6] This section is based on CNIL's privacy risk methodology (Nov 2012).

- A *primary asset* is anything that has value (not necessarily monetary) to an impacted party (whether individual or organisation) and which thus needs protection. Primary assets can be tangible and/or intangible, e.g., one's privacy, dignity and reputation can be regarded as assets. Primary assets could be valued by determining the cost or difficulty of replacing the asset as well as the consequences on the impacted organisation, individuals, groups and society if the asset is damaged or compromised. For a list of primary assets, see Annex on page 67.

- A *feared event* is anything that may have a negative effect on a primary asset, e.g., the false accusation of an innocent person, the loss of dignity for individuals subjected to a body scanner or the blanket categorisation of a particular population group as "high risk".

- A *supporting asset* is an information system or organisational component on which a primary asset relies, e.g., software (a database), hardware (a physical machine), a person (an administrator) or a printed document (a form).

- *Threats* may be accidental or deliberate, of natural or human origin. They may originate from within or outside the organisation. Examples of threats can be found in the annex (page 69) as well as in other threat catalogues.[7]

- Threats exploit *vulnerabilities* causing harm to stakeholders and their assets. See annex on page 72 for examples of vulnerabilities.

- A *threat source* is a person or organisation or natural event capable of exploiting a vulnerability.

- The *consequence* of a threat is the impact of exploiting a vulnerability. This could be a loss of business, damage to reputation, undermining effectiveness, etc. ISO 27005 describes this as an "incident scenario". The consequence of surveillance may be felt by individuals, groups, organisations (both the surveilled organisation as well as the surveilling organisation) and society as a whole. See annex on page 73 for examples of consequences.

- A *risk* is the probability or likelihood of a consequence arising from a threat exploiting an asset's vulnerability. Threats typically apply to supporting assets, which then indirectly affect a primary asset.

- We can assign a *severity* to risks in order to prioritise dealing with them.

Having identified relevant risks, the organisation should identify how it intends to treat those risks, i.e., which *controls* (or *countermeasures* or *safeguards*) will mitigate those risks? The risk treatment may involve reducing, eliminating, transferring or insuring against those risks.

The principal steps in the process of assessing risks from surveillance are outlined in Steps 8 and 9 in the SIA.

[7] For example, OSA (Open Security Architecture) is developing a threat catalogue. See http://www.opensecurityarchitecture.org/cms/en/library/threat_catalogue. The German Federal Office for Information Security (BSI) has produced several iterations of threat catalogues. See https://www.bsi.bund.de/EN/Topics/ITGrundschutz/Download/download_node.html.

3.3 *An overview of surveillance impact assessment*

A surveillance impact assessment (SIA) should be regarded as a *process*, comprising the following main steps.[8] The SIA *report* documents the process.

Some of the steps will be iterative. For example, the organisation conducting the SIA may identify some risks, and then consult with stakeholders who may identify some additional risks. Similarly, the organisation may identify some means of mitigating those risks and then consult stakeholders again, who may identify some other means of mitigation or alternatives to the way in which a proposed surveillance system is structured.

The specific steps followed and the attention (and resources) devoted to each step will be a matter of judgement and how credible the organisation responsible for the impact assessment wishes the report to be.[9] A high-level overview is given in figure 3.2 below, and illustrated in Figures 4.1, 4.2 and 4.8. The next chapter provides a more detailed step-by-step description. The list of the key steps for the SIA follows:

1. Determine if an SIA is necessary
2. Develop terms of reference
3. Prepare a scoping report (What is the scope of the surveillance system?)
4. Check compliance
5. Identify key stakeholders
6. Initiate stakeholder consultation
7. Identify risk criteria
8. Identify primary assets and feared events
9. Analyse the scope of feared events
10. Analyse the impact of feared events
11. Identify supporting assets
12. Identify threats and analyse vulnerabilities
13. Identify threat sources and analyse capabilities
14. Create a risk map
15. Risk treatment identification and planning

[8] This surveillance impact assessment guidance draws on Wright and Wadhwa, "A step-by-step guide to privacy impact assessment", ISO 27005, ISO31000, CNIL's privacy risk methodology, ENISA's risk management guidance, NIST 800-30 and EBIOS.

[9] Two examples, one from the private sector and one from the public sector, of well-conducted and credible privacy impact assessments are the following: Engage Consulting Limited, "Privacy Impact Assessment: Use of Smart Metering data by Network Operators", ENA-CF002-007-1.0, Energy Networks Association, London, 2011; Department of Energy and Climate Change (DECC), "Smart Metering Implementation Programme – Privacy Impact Assessment", London, 2012.

16. Prepare an SIA report
17. Record the implementation
18. Publish the SIA report
19. Audit the SIA
20. If necessary, update the SIA

Steps 1-5 comprise the preparatory phase. Steps 6-14 refer to the risk identification and analysis phase. Steps 15-19 refer to the risk treatment and recommendations phase.

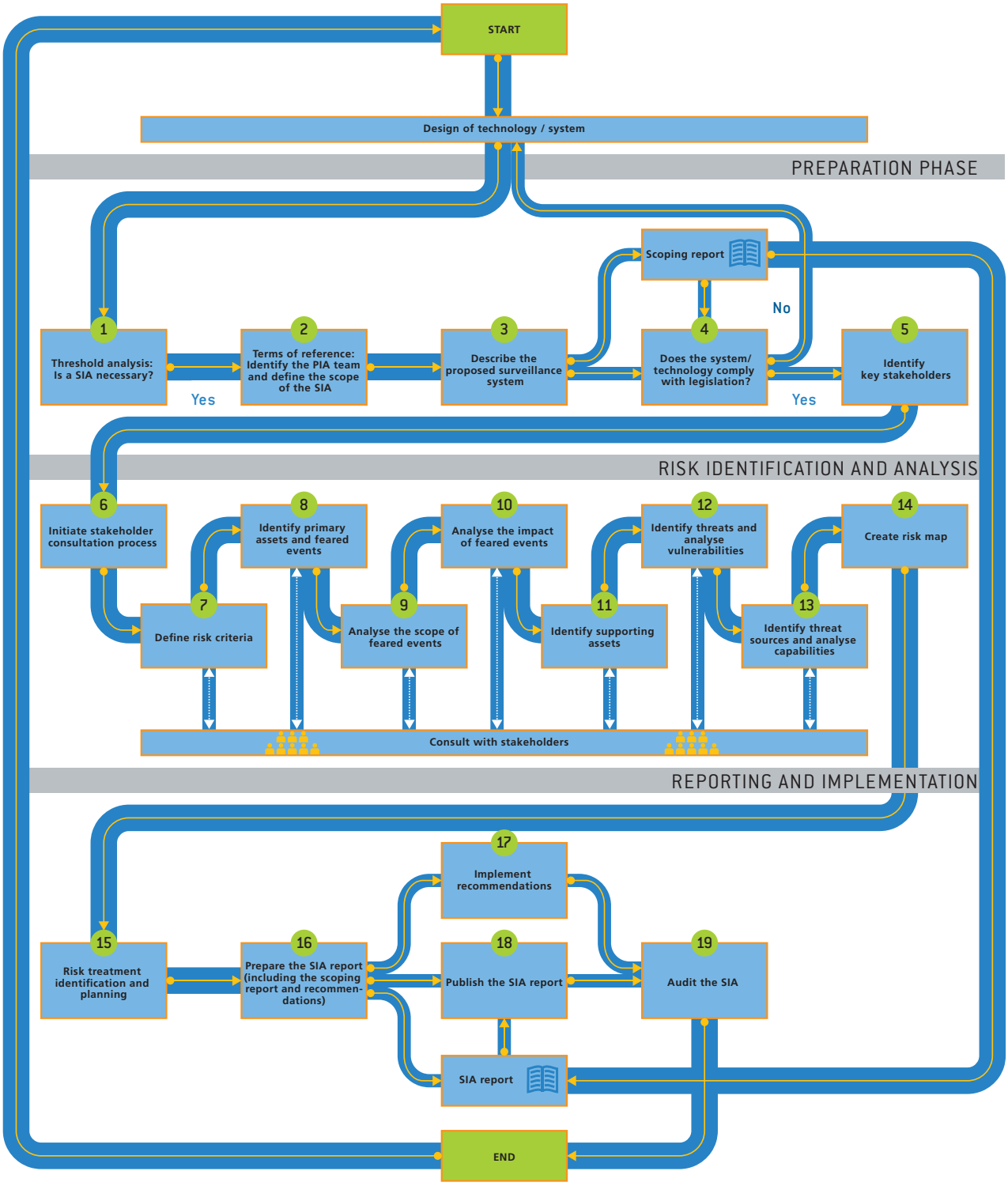


Figure 3.2: The Steps of a Surveillance Impact Assessment

4
Conducting a surveillance impact assessment

In this section, we present a step-by-step guide for SIA. We have designed the guide as a practical tool supporting organisations in their surveillance impact assessment efforts. In particular, the guide sheds light on the identification and analysis of surveillance risk.

4.1 Preparation

The following five steps describe the preparatory phase where the scope and objective of the SIA as well as its boundaries are discussed and defined (see Figure 4.1).

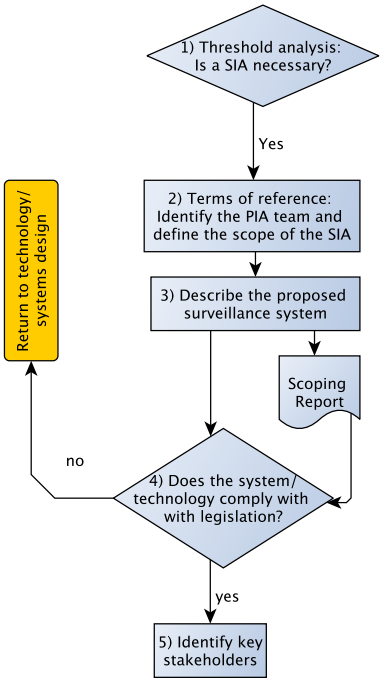


Figure 4.1: Steps 1–5 in the SIA

1. The first step is to determine whether an SIA is actually *necessary*. Generally, if an organisation is developing a surveillance technology or developing, deploying or operating a surveillance system, it should undertake an SIA. There may be some instances, e.g., involving national security or law enforcement, when an SIA may not be necessary or appropriate. In cases of doubt, the organisation should refer to the appropriate regulatory authority.

2. Identify the SIA team and set the team's terms of reference, resources and time frame. It is essential that appropriate resources are allocated to the conduct of a proper, credible SIA. A lack of resources will directly impact the quality of the SIA and may render the process useless. The project manager developing or deploying the surveillance technology or system should be responsible for the conduct of the SIA, but she may need some additional expertise, perhaps from outside her organisation. The assessor team could comprise the project manager or his delegate, a lawyer, a technical person, a communications expert (for engaging stakeholders), a financial expert (for analysing the cost-benefit of the

proposed system), an operations analyst, an ethicist, etc. These experts may or may not need to work full-time on the SIA, but they should be accessible to the assessor leading the SIA. The project manager and/or the organisation's senior management should decide on the terms of reference for the SIA team, i.e., to spell out who will conduct the SIA, its purpose, its budget, the time frame for its conduct, whether public consultations are to be held, to whom the SIA report is to be submitted, whether the SIA report is to be published, etc.

3. *Describe* the proposed surveillance system in a "scoping report". What types of surveillance will it involve? What is the scope and purpose of the surveillance technology, application or system? Why is the project being undertaken? What data will be collected? Who will have access to the data collected? Will the data be shared? How will the collected data be secured? Who comprises the target market? Who is responsible for the project? The description of the project should provide some contextual information. It should indicate important milestones and, especially, when decisions are to be taken that could affect the project's design. See Annex A for more questions which could be asked of a proposed surveillance system.

4. Check that the proposed surveillance system or technology *complies* with legislation. There may several different pieces of legislation of relevance (data protection, confidentiality of communications, surveillance, etc.). An SIA is more than a compliance check. Nevertheless, as a minimum, the project must comply with relevant legislation. As the SIA and, indeed, the project progresses, the assessor may need to revisit this step or may find other legislation or regulations that need to be checked.

5. Identify the *stakeholders* who should be involved in the SIA.[1] For whom is the surveillance system being developed? Who will be targeted by the surveillance system? Will it be targeted at specific individuals or groups or is it a mass surveillance system (e.g., CCTV cameras on the Underground or on buses or in the streets)? Who represents the stakeholders? How many people will be surveilled? The assessor should identify stakeholders, i.e., those who are or might be interested in or affected by the project, technology or service. Stakeholders could include people who are internal and external to the organisation. They could include regulatory authorities, customers, citizen advocacy organisations, suppliers, service providers, manufacturers, system integrators, designers, academics, the media and so on. The assessor should

[1] There are many reasons for engaging stakeholders, not least of which is that they may identify some privacy or ethical or societal risks not considered by the project manager or assessor. By consulting stakeholders, the project manager may forestall or avoid criticism that they were not consulted. If something does go wrong downstream – when the project or technology or service is deployed – an adequate consultation at an early stage may help the organisation avoid or minimise criticism and perhaps liability. Furthermore, consulting stakeholders may provide a sort of "beta test" of the project or service or technology. Consulted stakeholders are less likely to criticise a project than those who were not consulted.

identify these different categories of stakeholders and then identify specific individuals from within each category, preferably to be as representative as possible. The range and number of stakeholders to be consulted should be a function of the privacy, ethical and societal risks and the assumptions about the frequency and consequences of those risks. As the SIA progresses, the assessor may realise that additional stakeholders should be invited to participate in the process.

4.2 *Risk identification and analysis*

This phase focuses on risk identification and analysis. The purpose of *risk identification* is to determine which *feared events* could happen that would have negative *consequences* for the primary assets of *stakeholders*, and where, how and why this might occur.[2] This also includes assessing the *scope* of a feared event, i.e., the size of the population that might be affected by this event. *Risk analysis* is the process whereby the risk manager attempts to assess and understand the level of a risk and its nature.

[2] By impact, we refer to the potential consequence or impact on privacy and other human rights as well as on social or ethical principles (and the violation thereof). Impacts (consequences) can be on individuals, groups, organisations or society as a whole.

Not all risks carry the same seriousness or consequences or likelihood. In order to evaluate these risks and to formulate counter-strategies, values can be assigned to primary assets, threats, vulnerabilities and consequences.[3] The following sections describe how this can be done.

[3] The text and tables in this Annex have been adapted from CNIL (Commission Nationale de l'Informatique et des Libertés), "Methodology for Privacy Risk Assessment: How to implement the Data Protection Act", Paris, 2012, [pp. 12-16].

We have two identification-analysis cycles – first for the feared events, then for the threats that may lead to the feared events. The following are the key tasks in this step (see Figure 4.2; the individual steps are explained in more detail in the following sections):

- Identify the risk criteria, i.e., the criteria to use for evaluating the seriousness of the risk.
- Identify feared events. Stakeholders should play a major role in this.
- Analyse the severity (scope and consequences) of the feared events with a focus on the most important (this might eliminate some of the events that aren't that feared).
- Identify supporting assets for the remaining feared events, and the threats to these assets. Again, stakeholders can provide important input in this step.
- Analyse the likelihood of those threats (based on the vulnerability of assets and capabilities of threat sources).
- Create a risk map.

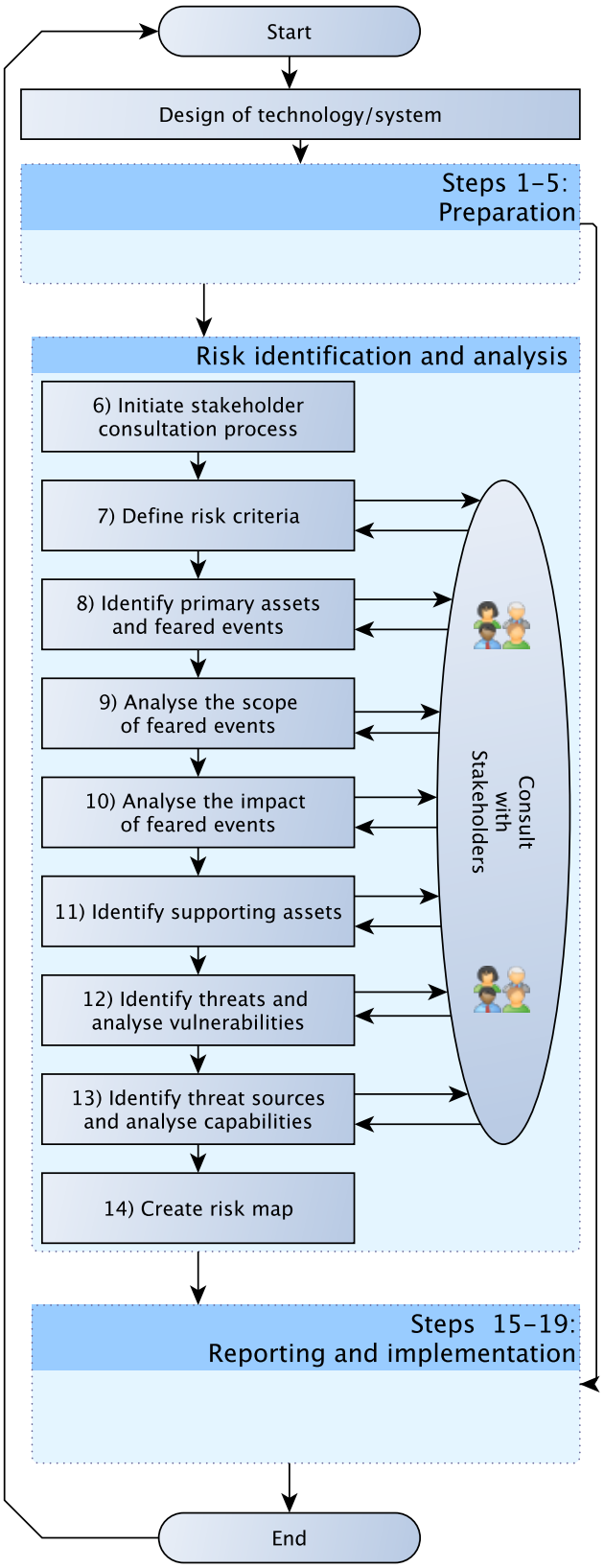


Figure 4.2: Steps 6-14 in the SIA

4.2.1 Consult stakeholders

Risk identification and analysis should be done in close consultation with the set of stake-holders identified in step 5.

6. Consult stakeholders so that they can contribute to the process of identifying and analysing risks. Gather stakeholder views on the primary assets (tangible and intangible) that should be considered in the SIA. The feared events may compromise these primary assets. Stakeholders can help identify the vulnerabilities of any supporting assets that these feared events may exploit. Stakeholders can also help identify and assess the threat sources aimed at exploiting vulnerabilities. A variety of consultation techniques could be used, including surveys, workshops, focus groups, Delphis, etc.

Consulting stakeholders will help to gauge the nature and intensity of their concerns and views with regard to the risks to the assets under consideration, and their reaction and input to possible options (outlined in the scoping report) for treating the risks. The scoping report, prepared in step 3, as well as the compliance check in step 4, can form the basis for consultation with stakeholders.

There are different approaches to stakeholder involvement.[4] We recommend initiating the process by conducting *focus groups*.[5]

Focus groups are planned discussion among a small group (4-12 persons) of stakeholders facilitated by a skilled moderator and designed to obtain information about (various) people's preferences and values pertaining to a defined topic and why these are held by observing the structured discussion of an interactive group. Focus groups are particularly useful when participants' reasoning behind their views is of interest, as well as the process by which participants' develop and influence each other's ideas and opinions in the course of discussion. The method is particularly useful when one is interested in complex motivations and actions, when one will benefit from a multiplicity of attitudes, when there is a desire to see what the prospects might be for consensus on a topic and whether there is a knowledge gap regarding a target audience.[6]

To prepare for the focus group events, the assessor first has to determine the questions to be addressed by the focus group. This should be done in steps 3 and 5. Then, the group participants need to be recruited. It is essential to engage representatives from all relevant stakeholder groups. Focus groups are rather short events of three to five hours (a half-day). The moderator leads the group through a semi-structured discussion to draw out the views of all of the participants and then summarises all of the main issues and perspectives

[4] For an introduction to the strengths and weaknesses of different methods and for guidelines on how to implement them, see, for instance: Slocum, Nikki, Stef Steyaert and Robby Berloznik, *Participatory Methods Toolkit: A practitioner's manual*, King Baudouin Foundation, Brussels, 2006.

[5] Since focus groups are common in marketing research and usability engineering, a company should be able to easily find a facilitator for this kind of stakeholder involvement.

[6] Dürrenberger, Gregor, Jeannette Behringer, Urs Dahinden, et al., "Focus Groups in Integrated Assessment: A manual for a participatory tool", ULYSSES Working Paper 97-2, Darmstadt University of Technology, Center for Interdisciplinary Studies in Technology, Darmstadt, 1997.

expressed. The group discussion will be initiated by a short pointed presentation of the surveillance technology or system to be assessed. The discussion should be recorded (with the agreement of the participants) to enable a systematic analysis and documentation of the focus groups.[7]

[7] Krueger, Richard A., Systematic Analysis Process. http://www.tc.umn.edu/~rkrueger/focus_analysis.html

4.2.2 *Establish risk criteria*

Those involved in the surveillance impact assessment should agree an initial set of risk criteria. Identifying and analysing risks is an iterative process, so after an initial analysis has been performed, the risk criteria might be revisited and re-aligned for a second iteration, and so on.

7. Risk criteria are those criteria by which risks will be evaluated. The organisation has to agree the criteria for deciding how to treat the risks, which are usually based on operational, technical, financial, regulatory, legal, social or environmental criteria or on combinations of these criteria. The main risk criteria considered in this guide are:

   - impact criteria and the consequences to be considered
   - likelihood criteria
   - the rules that will determine whether the risk level is such that further treatment activities are required.

Other risk criteria are possible. One could additionally (or alternatively) assess how easy or difficult it would be to turn off or dismantle the surveillance system or how likely "function creep" will be in the system.

The risk criteria are used in steps 8 and 9 in the SIA process.

4.2.3 *Identify and analyse feared events*

The focus of this step is feared events. As mentioned above (page 19) a *feared event* is anything that may have a negative effect on a primary asset, e.g., the false accusation of an innocent person, the loss of dignity for individuals subjected to a body scanner or the blanket categorisation of a particular population group as "high risk". Stakeholders can help identify feared events and what might happen to this primary asset if a feared event should occur.

See annex on page 67 for examples of primary assets. There are various ways to identify these and other primary assets. The scoping report forms the starting point for the engagement of stake-holders, including civil society, with the objective to consider key concerns

and issues related to the future use of smart surveillance systems from different perspectives.

The basis for our risk analysis is feared events. On the basis of the scoping report prepared in step 3, one needs to identify stakeholders' *primary assets* and the *feared events* that may happen to these assets (cf. Figure 4.3). As also mentioned above (page 18), a primary asset is anything that has value (not necessarily monetary) to an impacted party (whether individual or organisation) and which thus needs protection. Primary assets can be tangible and/or intangible, e.g., one's privacy, dignity and reputation can be regarded as assets. Primary assets could be valued by determining the cost or difficulty of replacing the asset as well as the consequences on the impacted organisation, individuals, groups and society if the asset is damaged or compromised. For a list of primary assets, see annex on page 67. As noted above, a supporting asset is an information system or organisational component on which a primary asset relies, e.g., software (a database), hardware (a physical machine), a person (an administrator) or a printed document (a form).

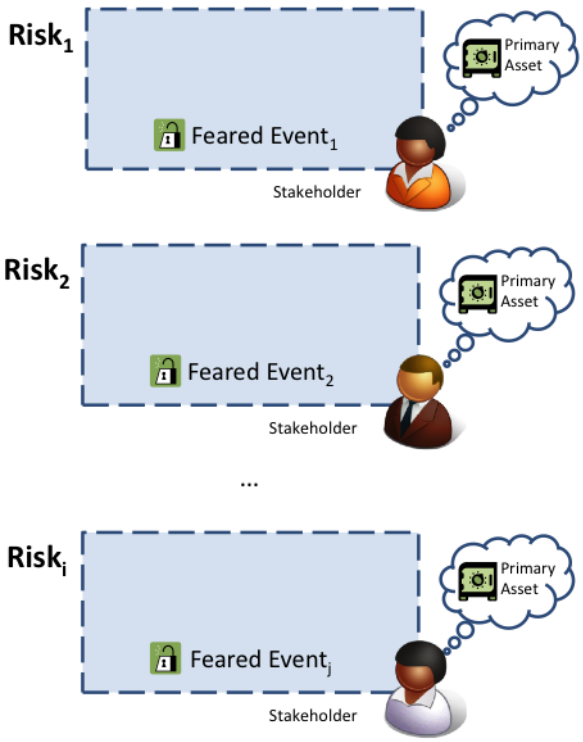


Figure 4.3: Feared events form the basis of the risk analysis process

8. *Feared events* may be accidental or deliberate, of natural or human origin. They may originate from within or outside the organisation. Note that we differentiate between a feared event and a threat. Examples of threats can be found in III on page 69 as well as in

other threat-related catalogues.[8] Threats are only considered in step 12 onwards, after the primary assets and the feared events have been identified and analysed.

9. For each of the feared events identified in step 8, the assessment team and/or stakeholders should make an assessment of **how many people** (organisations or groups) might be affected by the feared event under consideration
   - *Negligible*: Very few people (organisations or groups) will be affected by the feared event.
   - *Limited*: Some people – perhaps some specific groups – will be affected, but not that many as a percentage of the population
   - *Significant*: A large number of people will be affected – not everybody, but still a large percentage of the population.
   - *Maximum*: The whole of society, effectively everyone, will be affected.

Each of the team members should assign a value according to their assumptions about the number of people who will be surveilled – negligible is assigned a value of 1, limited a value of 2, significant a value of 3 and maximum a value of 4. Team members should assign these values individually, and after each has done so, each can reveal the number she assigned. Team members can discuss differences to see if they can reach a consensus or the assessor can simply take a numerical average or median (the latter would deal better with outliers). If there are, say, five team members, they might have assigned values of 3, 4, 2, 3 and 3 (for an average and median of 3).

10. Next, the assessment team should consider the consequences (impacts) of the feared event under consideration. In other words, how much damage[9] would be caused by the feared event on individuals, groups, organisations and society?
    - *Negligible*: Individuals, groups, organisations and society either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
    - *Limited*: Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
    - *Significant*: Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks,

[8] For example, OSA (Open Security Architecture) is developing a threat catalogue. See http://www.opensecurityarchitecture.org/cms/en/library/threat_catalogue. The German Federal Office for Information Security (BSI) has produced several iterations of threat catalogues. See https://www.bsi.bund.de/EN/Topics/ITGrundschutz/Download/download_node.html. In these catalogues, a "threat" may be what we consider a "feared event" in the context of an SIA.

[9] Damage to individuals may be: physical (loss of amenity, disfigurement or economic loss related to physical integrity), material (loss incurred or lost revenue with respect to an individual's assets), moral (physical or emotional suffering, disfigurement or loss of amenity, etc.).

property damage, loss of employment, subpoena, worsening of state of health, etc.).

- *Maximum*: Individuals may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).

Again, each member of the assessment team should assign a value from one to four according to the level that she thinks best matches the potential impacts of the feared event. After each person in the assessment team has assigned a value, they may wish to discuss their values and see if they can reach a consensus. Otherwise, a numerical average can be used. In this case, the five team members might assign values of 4, 5, 4, 3, 2 and 4, which equates to an average of 4.4 or a median of 4.

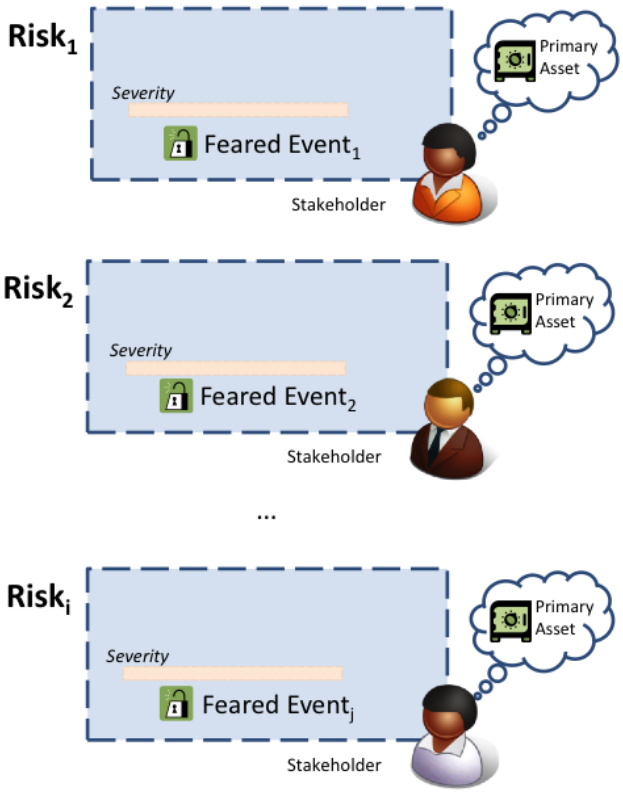


Figure 4.4: We can assess the "severity" of each feared event by combining its scope with an assessment of its consequences

Finally, the consequence (or impact or severity) is determined by adding the consensus number or numerical average regarding the numbers of people affected plus the consensus number or numerical average regarding the prejudicial effects or potential impact values obtained and locating the sum in the table below (cf. also Figure 4.4).

[10] Negligible here means a minimal number of people are affected. It is not intended to downplay the seriousness of a risk to just one person or just a few.

Numbers of people affected + impacts	Corresponding severity
< 5	1. Negligible[10](= minimal)
= 5	2. Limited
= 6	3. Significant
> 6	4. Maximum

Table 4.1: Determining the *severity* (consequence or impact) of each risk

Using our example above, one could add the two means of 3 + 4.4 = 7.4, which would indicate that the corresponding severity is "Maximum".

4.2.4 *Identifying and analysing threats*

Identifying what may happen and to whom is rarely sufficient. The fact that there are many ways in which an event can occur makes it important to examine all significant causes and scenarios and perform a *threat analysis*. In this step, the aim now is to obtain a detailed, prioritised list of all threats that may allow a feared event to occur. It is possible to leave out threats relating to feared events of negligible (1) or limited (2) severity.

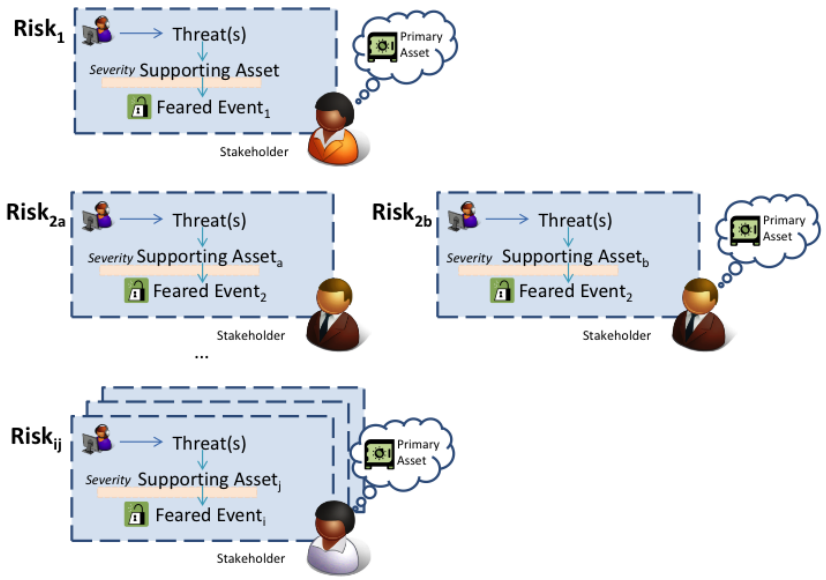


Figure 4.5: Identifying threats to supporting assets, and their corresponding threat agents

11. Since a threat is a possible action by a threat source on *supporting assets*, the supporting assets should first be identified (cf. Figure 6). If one fears an attack on one's dignity by the spread of nude images taken from a body scanner, the primary asset would be

"dignity" while the supporting asset would be the database and/or imaging component of the body scanner.

12. Next, we need to identify *threats* to these supporting assets (cf. Figure 7) and to estimate their *vulnerability* to these threats. In other words, to what degree can a threat exploit the vulnerabilities? For example, we might want to know what are the vulnerabilities of a video stream taken by a CCTV camera system.

    - *Negligible*: Carrying out a threat by exploiting the assets does not appear possible (e.g., the CCTV system does not store any video and is not connected to a network).
    - *Limited*: Carrying out a threat by exploiting the properties of assets appears to be difficult (e.g., the CCTV system does not record a video stream but is connected to the network, so an attack might intercept the signal).
    - *Significant*: Carrying out a threat by exploiting the properties of supporting assets appears to be possible (e.g., the CCTV system stores video streams for extended periods of time, and/or is connected to public networks).
    - *Maximum*: Carrying out a threat by exploiting the properties of supporting assets appears to be extremely easy (e.g., the CCTV system's video stream is available via an unsecured Web interface).

Each member of the assessment team selects a value from one to four that that best corresponds to how vulnerable she thinks the supporting asset is. When each team member has done so, they can reveal their selections to each other and discuss them. The discussion is potentially important because team members may have differing views on what the role of a supporting asset is for any of the "primary assets" under consideration, such as privacy, dignity, reputation, freedom of expression, etc. As before, the team members should either reach a consensus or choose to take the numerical average (or median) of their selections. These might be 1, 2, 3, 2 and 1, which would give an average score of 1.8.

13. Next, the team members should estimate how serious the threat is. What are the *capabilities of a threat source*, sometimes known as the risk agent, to exploit vulnerabilities (skills, available time, financial resources, proximity to system, motivation, feeling of impunity, etc.) of any supporting asset for the primary assets in question? For example, the team members might consider how capable a burglar might be in attacking the CCTV system (for the feared event of finding an apartment to break into).

- *Negligible*: The risk agent does not appear to have any special capabilities to carry out a threat (e.g., the typical burglar isn't well versed in breaking into a computer system).
- *Limited*: The capabilities of a risk agent to carry out a threat are limited (e.g., as the CCTV system's unsecured Web access appears in a public Web search, a burglar might happen to find it, as he or she knows the right search string).
- *Significant*: Carrying out a threat by exploiting the properties of supporting assets appears to be possible (e.g., the CCTV system stores video streams for extended periods of time, and/or is connected to public networks).
- *Maximum*: Carrying out a threat by exploiting the properties of supporting assets appears to be extremely easy (e.g., the CCTV system's video stream is available via an unsecured Web interface).

Each of the team members then repeats the exercise, as previously, by selecting a value from one to four that best corresponds to their assumptions about the capabilities of the risk source. And, as before, the team members may wish to discuss their assumptions about the capabilities of the risk source in order to reach a consensus value, or simply take the numerical average or median. So if the five team members selected scores of 2, 3, 2, 4 and 2, the average would be 2.6 (and the median would be 2).

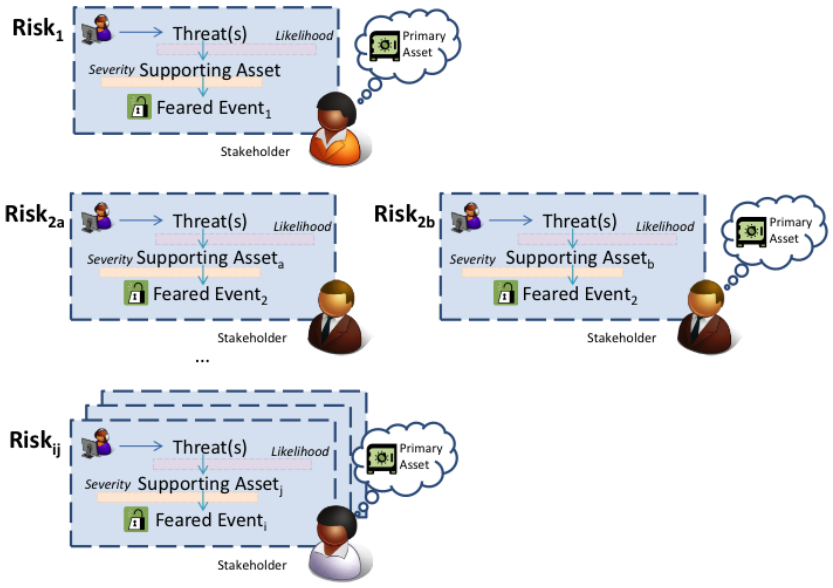


Figure 4.6: Estimating the likelihood of a threat, based on the vulnerability of a secondary asset and the capabilities of a threat source

Finally, the likelihood of the threat is determined by adding the values assigned to the vulnerabilities of the assets and the values assigned to the capabilities of the risk source and locating the sum in table 4.2 below:

Table 4.2: Determining the *likelihood* of each risk

Vulnerabilities + threats	**Corresponding likelihood**
< 5	1. Negligible (= minimal)
= 5	2. Limited
= 6	3. Significant
> 6	4. Maximum

In our example, the average values of 1.8 and 2.6 would add up to 4.4, which would equate to a negligible likelihood.

4.2.5 *Creating the risk map*

Methods and tools used to analysis risks and their occurrence include checklists, judgements based on experience and records, flow charts, brainstorming, systems analysis, scenario analysis and systems engineering techniques. Analysing risks is a somewhat subjective exercise. Therefore, it is important to have a balanced and representative selection of stakeholders engaged in the process.

14. The aim of this step is to evaluate the risk and obtain a risk map in order to determine the order in which risks should be treated.[11] Risk evaluation is the process of comparing the results of risk analysis with the risk criteria to determine whether the risk is acceptable or tolerable. During the risk evaluation phase, the organisation must decide which risks to treat and which not to, and their priorities for treatment. Analysts and/or the SIA team need to compare the level of risk determined during the analysis process with the risk criteria, which should take into account organisational objectives, stakeholder views and the scope and objectives of the risk management process itself.

[11] The text and figure have been adapted from CNIL (Commission Nationale de l'Informatique et des Libertés), 2012, [p. 18-19].

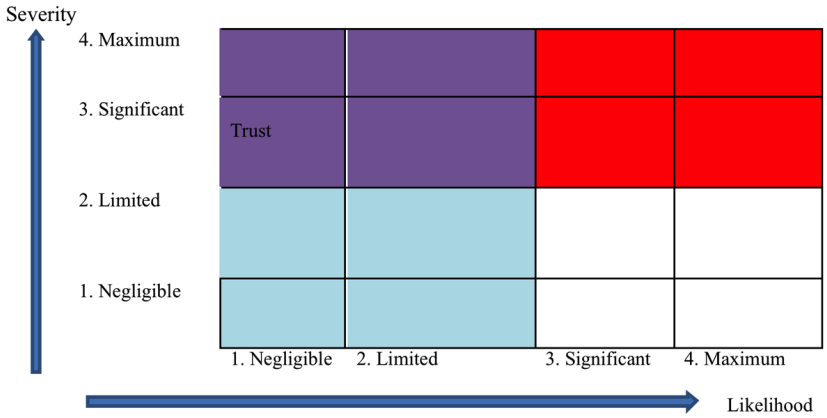
In the process described below (figure 4.7), the decisions are based on the level of risk in terms of:

- *severity* of the feared event: what would be the scope and what would be the consequence of the feared event happening?
- *likelihood* of the feared event: how capable is the threat source to exploit a vulnerability of an asset?

Additional evaluation parameters might include the cumulative impact of a series of events that could occur simultaneously or over some period of time.

Example: A risk is classically equated with its consequence or impact or severity times its likelihood, as depicted below. Using the example scores from step 10, we had a maximum severity but a negligible likelihood of a break-in (primary asset: valuables, cash, documents, but also personal safety and well-being), based on a hacked CCTV system. We can repeat the exercise for other primary assets, too, e.g., dignity, reputation, freedom of expression, etc., and they will likely fall elsewhere on the risk map. The most serious risks (those that fall within the red quadrant) will be those that should be given priority attention – to take some measures to avoid, eliminate, reduce or transfer those risks.

Figure 4.7: Risk map



Locating risks on the map helps the risk management team determine the order of priority in which risks should be treated and strategies can be formulated accordingly taking the following factors into account:

- Risks with a high severity and likelihood absolutely must be avoided or reduced by implementing measures that reduce both their severity and their likelihood. Ideally, care should even be taken to ensure that these risks are treated by independent measures of prevention (actions taken prior to a damaging event), protection (actions taken during a damaging event) and recovery (actions taken after a damaging event).
- Risks with a high severity but a low likelihood must be avoided or reduced by implementing measures that reduce either their severity or their likelihood. Emphasis must be placed on preventive measures.

- Risks with a low severity but a high likelihood must be reduced by implementing security measures that reduce their likelihood. Emphasis must be placed on recovery measures.
- Risks with a low severity and likelihood may be accepted (e.g., CCTV on public buses), especially since the treatment of other risks should also lead to their treatment.

4.3 *Risk treatment and recommendations*

This phase deals with the identification and implementation of the measures to treat the evaluated risks as well as the key reporting. It comprises the following steps (see figure 4.8):

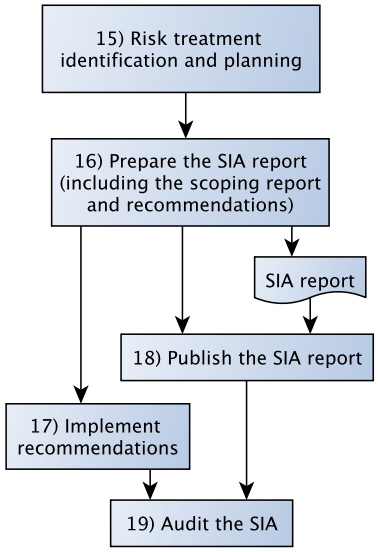


Figure 4.8: Steps 15-19 in the SIA

15. *Plan risk treatment*, which is the process of selecting and implementing measures to treat risks. Treatment options are avoiding, optimising (or minimising or modifying), transferring (or sharing) or retaining risk. Not all risks present the same probability of negative impacts; some risks may present opportunities. The risk manager should compare the cost of managing a risk with the benefits obtained or expected. It is important to consider all direct and indirect costs and benefits, whether tangible or intangible, and measured in financial or other terms. Treatment plans should describe how the chosen options will be implemented and should provide all necessary information about:
    - proposed actions, priorities or time plans
    - resource requirements
    - roles and responsibilities of all parties involved in the proposed actions
    - performance measures
    - reporting and monitoring requirements.

Regarding risk treatment, decide how to mitigate or eliminate or avoid or transfer the risks posed by the surveillance system. This is a somewhat political decision as is the decision regarding which risks to retain. The assessor may even wish to consider possible alternatives to the proposed surveillance system – or at least to part(s) of the system for which this is feasible. Be as broad as possible in the consideration of options. The following may be useful questions in this regard – but are certainly not exhaustive: Which parts of the system are strictly necessary? Can the scale of the proposed surveillance system be reduced? Can oversight of the system be improved? Is it possible to consider scrapping the system altogether? The alternatives considered should take into account the risk consideration

exercise as well as the stakeholder consultation. This step necessarily includes a feasibility study of the treatment.

16. Prepare a surveillance assessment *report*, which would include the scoping report prepared in step 3 as well as the results of the other steps. The report should include a set of *recommendations*. The assessor should be clear to whom her recommendations are directed – some could be directed towards different units within the organisation, some to the project manager, some to the CEO, some to employees or employee representatives (e.g., trade unions), to regulatory authorities, third-party apps developers, etc. If stakeholders have sight of draft recommendations, before they are finalised, they may be able to suggest improvements to existing recommendations or make additional ones. The name and contact details of the person who prepared the report should be on the cover page.

17. *Implement* the report's recommendations or, if some recommendations are not adopted, the organisation should state why it does not intend to implement particular recommendations in a short report to be posted on the organisation's website and to accompany the SIA report.

18. *Publish* the report on the organisation's website. If there are commercially sensitive or security sensitive issues, these can be redacted or put in a confidential annex. The decision to make part of the report confidential should not be done arbitrarily, but should be based on legitimate grounds. Every effort should be made to elaborate the reasons for the decision to withhold information in the report. If possible, a trustworthy third party should be involved to confirm the legitimacy of the decision to withhold. Alternatively, a summary of the report could be posted on the organisation's website. Whichever approach is decided should be subject to audit (step 12). The organisation should create an index or register of SIA reports, i.e., a single webpage where website visitors can find all of its SIA, PIA and/or other impact assessment reports. If necessary, and if possible, the report should also be submitted to the relevant supervisory authority – this may be the national data protection authority (DPA).

19. Subject the SIA report to independent, third-party review or *audit* to make sure that the SIA was carried out properly and that the recommendations have been implemented, unless the organisation intends not to carry out some recommendations as stated in step 9.

20. If significant changes are made to the surveillance system or technology after the report has been prepared, the SIA should be updated or repeated.

5
Conclusion

This guide has formulated a set of principles that should govern the development and deployment of surveillance technologies, systems and applications as well as the conduct of a surveillance impact assessment. The SAPIENT consortium has had numerous discussions and has drawn on different sources in the development of this guide. The consortium has also sought the views of various experts, some of whom are acknowledged below, on the draft guide, and we will be testing the guide in some field trials of surveillance impact assessment and, depending on the results, further refining the guide. Some of the sources upon which we have drawn use different terminologies (e.g., impacts, consequences; controls, counter-measures, mitigating measures, safeguards), and we have sought to put in parentheses where different terminologies are current in the world of risk assessment. While we have set out a step-by-step process for the conduct of an SIA, each project manager or assessor will need to decide what is appropriate in his or her own case. In some cases, the SIA could be streamlined, in others, it could be more elaborated. Nevertheless, some elements are very important for the credibility of any SIA, notably, engaging stakeholders, publication of the SIA report and independent, third-party review of SIA and the implementation of its recommendations.

Part II

Small-scale Surveillance Impact Assessment

6
Guide for a small-scale Surveillance Impact Assessment

6.1 Introduction

A surveillance system can raise risks for individuals, groups and organisations, as well as society as a whole. The purpose of a surveillance impact assessment (SIA) is to assess the risks a surveillance-related project, policy, programme, service, product or other initiative poses for privacy, as well as for other human rights and ethical values. The risk assessment addresses the *likelihood* of a certain event and its *consequences* (i.e., impacts). An SIA should include stakeholder consultation and, ultimately, lead to mitigating measures as necessary in order to avoid, minimise, transfer or share the risks. An SIA should follow a surveillance initiative throughout its lifecycle. The project should revisit the SIA as it undergoes changes or as new risks arise and become apparent.

The aim of this SIA is to create an initial risk map. Any organisation will face different types of risk. With regard to risks associated with new surveillance systems, the major risks arising in the area of privacy, data protection and ethics, include the following:

- Risk of a data breach
- Damage to reputation, e.g., the surveillance system is viewed negatively in the media and public opinion polls, which may affect the organisation's bottom line
- Disruptions to business continuity, e.g., dealing with the negative impacts of a surveillance system consumes undue amounts of an organisation time and may threaten the organisation's viability
- Risks arising from lack of compliance with legislation and/or other regulatory strictures

- Liability, e.g., the organisation may be sued for infringing the rights and freedoms of those surveilled.

By conducting an SIA, an organisation will be able to identify the risks involved in a project and begin to understand the nature of those risks (i.e., how likely, with what consequences, etc.). An important part of risk assessment is to determine who might be affected by the privacy or surveillance risk and how they might be harmed. This document will guide you through the steps you need to undertake to conduct a surveillance impact assessment. It should be read in conjunction with a questionnaire (see Annex, page 77) to be sent out to the stakeholders you identify.

6.2 Project description

As a first step, please provide a description of your project. This should include at least the following information:

- What are the main aims of your surveillance system or technology? Why is the system or technology being established?
- What are the principal features of your system or technology?
- What is its current status (i.e., not yet started, underway, completed)?
- When is your surveillance system expected to be operational?
- What is the expected outcome of your project (e.g., a demonstrator technology or a technology ready for market)?
- A description of the intended information flows of the project. This description should outline what sort of information or data will be collected. Will this data be stored? Will this data be processed? Will this data be transferred or communicated?

Please also include any other details that you feel are relevant or useful for an assessment of your project, including the benefits of the surveillance system or technology. This project description should be sent out to all relevant stakeholders. Following the description, you could include some questions aimed at gathering stakeholder views on the benefits you have identified of your system or technology, the perceived risks and their views on possible solutions.

6.3 Identifying Stakeholders

As a second step, please identify any internal or external stakeholders whom you feel should be included in the SIA process. This is

an important part of conducting a surveillance impact assessment. Involving a variety of stakeholders provides an opportunity for any potential risks to be highlighted and eventually managed. The earlier a consultation process is entered into, the more benefits an organisation can expect to draw from it. Examples of internal stakeholders are: the project management team, engineers, designers and developers, potential suppliers and data processors, customer-facing roles, legal staff, public relations staff, the data protection officer and senior management. Examples of external stakeholders are data protection authorities, civil society organisations (privacy advocates), academics, the media, members of the public, other businesses (e.g., manufacturers, suppliers, third-party service providers).

6.4 The Questionnaire

As a third step, the questionnaire (see Annex, page 77) should be sent out to internal stakeholders. The questionnaire is split into three sections. The first part is to identify risks associated with the project in the areas of legal compliance, other privacy issues, and ethical and social considerations. The second part of the questionnaire asks internal stakeholders to map the risks they have identified according to the likelihood and impact of an event happening.

The current EU Data Protection Directive 95/46/EC contains the following eight principles that must be followed in order for a surveillance system to be legally compliant:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate
5. Not kept for longer than necessary
6. Processed in accordance with individual's rights
7. Secure
8. Not transferred to countries without protection

The first section of the SIA questionnaire is based on the eight data protection principles outlined above. These questions will help to identify areas of risk in relation to the legal compliance of a project. The remaining questions aim to help an organisation identify other types of risk associated with new surveillance systems. These questions can be modified to suit the needs of your project. They are

included in the questionnaire to provide guidance on the types of questions that could be asked. The aim of the SIA is to include, but also to move beyond compliance with the data protection principles outlined previously, to also include the wider social and ethical implications of new surveillance systems.

The next stage in an SIA is to contact external stakeholders. The results of the risk assessment conducted with internal stakeholders can be used to inform a set of questions to be sent out to external stakeholders. The aim of consulting with external stakeholders is to gain their opinions on the risks associated with the project, the proposed solutions, and the benefits of the system, technology or application. The organisation should include a brief description of the project with the questionnaire, including any benefits that are foreseen in relation to the project.

6.4.1 The Risk Map

In the questionnaire, (internal and/or external) stakeholders are asked to complete a risk mapping exercise, in which the risks identified are mapped in relation to likelihood and impact. Locating risks on the map helps to determine the order of priority in which risks should be treated and strategies can be formulated accordingly taking the following factors into account:

- Risks with a high severity and likelihood absolutely must be avoided or reduced by implementing measures that reduce both their severity and their likelihood. Ideally, care should even be taken to ensure that these risks are treated by independent measures of prevention (actions taken prior to a damaging event), protection (actions taken during a damaging event) and recovery (actions taken after a damaging event).

- Risks with a high severity but a low likelihood must be avoided or reduced by implementing measures that reduce either their severity or their likelihood. Emphasis must be placed on preventive measures.

- Risks with a low severity but a high likelihood must be reduced by implementing security measures that reduce their likelihood. Emphasis must be placed on recovery measures.

- Risks with a low severity and likelihood may be accepted (e.g., CCTV on public buses), especially since the treatment of other risks should also lead to their treatment.

6.4.2 Solutions

The final section of the questionnaire asks (internal and/or external) stakeholders to identify solutions to the risks identified. The outcome of any solution is mapped against the criteria of whether the risk will be avoided, minimised, transferred or shared. The results of this section should enable an organisation to develop a plan to select and implement measures to treat risks. Treatment options are avoiding, optimising (or minimising or modifying), transferring (or sharing) or retaining risk. Treatment plans should describe how the chosen options will be implemented.

6.5 Preparing a surveillance assessment report

Organisations should publish a report containing the results of the surveillance impact assessment. Publishing the results of the SIA can improve transparency and build public trust with regard to how information about individuals is collected, stored, processed and transferred. The report should include the background information provided to stakeholders, the outcome of the assessment in terms of risks and solutions identified, and a set of recommendations and how these will be adopted by the organisation.

Part III

Annex

Criteria and Questions

Impacts of surveillance systems

Surveillance systems can have a range of impacts such as the following:

- Surveillance may have impacts on all (seven) types of privacy[1] (e.g., being subjected to unsolicited marketing telephone calls, being videoed every time one talks to a friend in a bar, being tracked wherever one drives one's car or every time one turns on one's computer, being forced through a body scanner, etc.).
- Surveillance may have an impact on a range of other human or fundamental rights. For example, the right to freedom of expression or freedom of association. Surveillance may have social impacts and raise social issues. Surveillance may have impacts on essentiality (i.e., a surveillance system is widely regarded as essential to society and cannot be turned off, e.g., video surveillance systems in an airport).
- Surveillance may have political impacts and raise political issues (e.g., intelligence agencies that monitor our telephone, mobile and Internet activity without citizens knowledge may have some political "blowback", as President Obama and other political leaders have encountered since *The Guardian* began its series of exposés regarding the extent of the NSA's monitoring activities).
- Surveillance may raise legal issues in addition to privacy and data protection (e.g., discrimination, fair trial and the presumption of innocence).
- Surveillance may raise ethical issues. Have citizens given their informed consent to their being subject to constant, ubiquitous surveillance?

[1] Finn, Rachel L., David Wright and Michael Friedewald, 'Seven types of privacy', in Gutwirth, Serge, et al. (eds.), *European Data Protection: Coming of Age*, Springer, Dordrecht, 2013.

A surveillance system may have impacts on individuals as well as groups or society as a whole.

It is often infeasible or not necessary to address *all* potential impacts of a surveillance system. The assessor must thus decide which

of the above impacts are most relevant in a particular situation and focus the efforts accordingly.

The following section sets out questions that can be used to uncover risks raised by surveillance in relation to the various types of possible impacts: privacy impacts, societal impacts, economic impacts, political considerations, legal impacts, ethical impacts, psychological impacts and organisational impacts.

Questions re data protection

- Is information processed in any way?
- Is information linked or linkable to identifiable individuals?
  - If not, could this information be made non-identifiable (anonymous)?
  - Could it be made pseudonymous?
  - Is any sensitive information collected – e.g., concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life?
  - Is any other information collected, which could be regarded as sensitive, e.g., genetic information? Is sensitive information differentiated from other information collected?
  - Is data about children being collected? Are special rules in place for this data?
  - Is data relating to third parties extracted from individuals' personal data (social network analysis etc.)? Are third parties informed of this?
- Do you have a legitimate reason for processing personal data?
  - If the system relies on consent, is this consent valid? Is it freely given, specific, informed and explicit?
  - Is there a power imbalance present which could undermine the legitimacy of consent – in a work context, for example?
  - Can consent be withdrawn? If not fully, to what extent can it be withdrawn? To what extent can data be deleted and the individual "forgotten"?
  - If the system relies on another reason to process data, does this require a statutory basis? If so, is there a specific and clear law which justifies the surveillance activity?
  - Have you assessed whether there are any other regulatory requirements to which you may be subject, e.g., confidentiality?

If yes, can your system ensure that the standards imposed by these requirements are met?

- Can the system conform to the fair information practice principles, particularly as set out in European data protection law?
  - Is data processing done fairly and transparently to the data subject?
  - Are policies on access made easily available?
  - Is all information required by disclosure obligations in law communicated to the data subject? Is this communication done in a form understandable by the data subject?
  - When is the individual informed? Could the individual be informed earlier?
  - Is information about the individual collected from third parties? If so, is this legitimate and are the interests of the data subject protected?
  - Is the data being used for purposes other than those originally stated? Are these purposes compatible with the original purposes of processing? Are these purposes also legitimate? Is the data subject told about these purposes?
  - What power does the data subject have to prevent further processing?
  - Does data collected fit with the purpose of the system?
  - Could less data, or less sensitive data, be collected to achieve the same result?
  - For how long are data stored? Is this length of storage strictly necessary for achieving the aims of the system? How often will retention periods be reviewed? Is data deleted after the expiration of the retention period? If not, is the further retention legitimate?
  - Are data accurate and kept up to date?
  - What level of accuracy is achieved by the system? Are there quality control checks foreseen? Is the data subject involved in these?
  - Are facilities in place to correct, delete or assess disputed or inaccurate data?
  - If data have been passed on to third parties, are procedures in place for communicating any rectification or deletion to those third parties?
  - Can the system controller ensure responsibility for the intended processing of data?

  - Can the controller ensure compliance with data protection obligations?
  - If other controllers are involved, is responsibility divided effectively between them?
  - If other data processors are involved, has the controller ensured they maintain compliance with data protection legislation, and with the processing rules laid out by the controller?
- Does the system allow the exercise of the rights of the data subject?
  - Does the system foresee procedures for the data subject to exercise his or her rights?
  - Can the data subject obtain confirmation of whether his or her personal data are being processed?
  - Is all relevant information relating to this confirmation provided to the data subject? If not, are there legitimate reasons for this?
  - Does the data subject have to pay a fee for gaining access to his or her personal data?
  - Is there the possibility to rectify or erase the data?
  - Is the individual profiled? Is there a legitimate ground for this profiling? How transparent is this profiling? Is there any information relating to this profiling to which the individual cannot gain access?
- Can the controller fulfil data protection obligations?
  - Have data protection principles been taken into account in the design and construction of the technical and organisational aspects of the surveillance technology or system?
  - Which data security measures have been put in place? Are these effective and adequate? Do they adhere to any appropriate standards?
  - Where necessary and relevant, have all relevant codes of conduct been followed?
  - Do any particular obligations emerge from sector specific rules or guidelines?
- Oversight requirements
  - Has a surveillance impact assessment of the surveillance system been carried out?
  - Does the system require prior checking with the data protection authority or privacy commissioner?

- Further disclosures of data
  - To whom (third parties) are data disclosed? Are transfers done on a legitimate basis?
  - Have these third parties been checked for their compliance with data protection principles?
  - Are any transfers outside the EU foreseen?
  - Do the countries or organisations to which the transfer is foreseen meet EU data protection standards? If not, is the transfer legitimised in any other way?
  - Are any services (e.g., cloud services) used that are not located in the EU? What assurances do the providers of these services offer that they will comply with EU data protection requirements?
- Massive collections of data
  - If massive data collection occurs, is there the chance that privacy interests may be affected – through aggregation, correlation, data matching, etc.?

Questions re other types of privacy

- Does the system process information on groups of people?
- Do these groups match to recognised social groups?
- Could these categories be regarded as discriminatory?
- Does the surveillance system seek to create groups or does the system work on the basis of pre-programmed groups?
- What is the evidence base for creation of these groups?
- Are these groups and the way they are created made transparent and available to these groups and the individuals within these groups?

Privacy of organisations

- Are the structures or internal secrets of organizations revealed through surveillance?
- Is the action of the surveillance system likely to impact on the function of any organisation or its ability to achieve its ends?
- Is the surveillance of the organisation likely to be known to the public?

- Might this have a negative effect on public perception of that organisation?

Anonymity

- Does the system surveil someone who would not have been under surveillance previously?
- Does this surveillance remove the possibility of anonymity?
- Through the use of anonymous data, does the system intend to have consequences for individuals, or groups, who would not qualify as data subjects?
- If anonymous information is used based on an original consent to process personal data, does this use raise issues to which the individual is likely object on moral grounds?
- Could more information be extracted from data which has been labelled as anonymous – on the basis of technological advance or in the context of a more advanced or thorough analysis?

Right to be let alone

- Is the individual subject to such surveillance that possibilities to seclude him or herself are reduced?
- Does this surveillance occur to such an extent that areas which would normally have been the individual's sole domain are also under surveillance?

Right to associate with others in private

- Is the aim of the system to surveil groups or gatherings of people? Is this focus legitimate? Does the surveillance system impede the gathering of individuals?
- Does the system make possible the revelation of the membership of groups?
- Does the system perceive as illegitimate gatherings that would previously have been considered legitimate?
- Does the system impact on the ability of individuals to form groups?
- Does the system shape the public space so that the practical ability to gather and associate is removed?

Right to freedom of expression and communication

- Does the system impact on the ability of groups or individuals to receive information? Does the system impact on the ability of groups or individuals to impart information?
- Does the system impact on the freedom of the media?
- Does the surveillance system impact on the public sphere, potentially altering, or chilling channels of information exchange and distribution?[2]
- Does the system focus on specific sorts or genres of communication?
- Are any individuals' communications monitored?
- What is the extent of this monitoring and why is it being conducted? Has such monitoring been properly authorised?
- Is the content of the communication revealed?

[2] The chilling effect occurs when people are more guarded in what they say or do because they are or believe they are under surveillance. The chilling effect is generally deleterious in a democracy where freedom of expression is a fundamental or constitutional right.

Right to free development of individuality and identity

- Does the surveillance system affect the development of individual identity?
- Does the system impose a change in individuals' identity?

Right to freedom of thought and religion

- Does the system affect the possibility to develop, or manifest, cultural or linguistic identity?
- Does the system seek to reveal individuals' thoughts, beliefs or religious identities? Does it focus particularly on certain religions as opposed to others?
- Does it work to the extent that it judges certain beliefs in a different way to others? Does it potentially prevent any religious manifestation – in terms of worship, teaching, practice or observance?

Right to travel without being tracked

- Does the surveillance system track the individual's movement across physical or cyberspace?
- Does this allow a picture of the individual's movements to be constructed?

Societal impacts

- Who authorised the system (e.g., Parliament or a local authority or the judiciary or the senior executive of a social network)?
- How was it authorised?
- Has the system been the subject of public scrutiny (if not consensus)? Specifically : Has any consent been given in relation to participation in the project, technology, application or service as a whole, and in particular features of it, rather than legal compulsion, or other forms of coercion?
- Does the project, technology, application or service sort individuals into groups according to some predetermined profile that may advantage some groups and disadvantage others?
- What is the accessibility and equity of the project, technology, application or services provided?
- What are the geographical equity impacts, e.g., do services differ according to location or access to facilities?
- What are the social equity impacts, e.g., do services differ according to ethnic background, linguistic skills, education or physical limitations?
- Does the surveillance in question have a negative impact on social cohesion and trust?
- Does the project, technology, application or service increase or decrease social affiliation or isolation?
- Does the project, technology, application or services increase or decrease social participation or passivity (citizens' involvement in management of public affairs)?
- Does the project, technology, application or service increase or decrease social acceptance or rejection?
- Does the project, technology, application or service increase or decrease legitimacy or illegitimacy of institutions that act as mediators, i.e., in representing people's)?
- Is the system actually the best way to achieve a given social objective (e.g., a reduction in violent crime or in benefits fraud)?
- What is the allocation of effort, costs and risks? Are they shifted in the direction of citizens?

- What are the choices in relation to the use of the project, technology, application or services provided as a whole, including benefits foregone if the system is not used?
- What are the potential impacts of the project, technology, application or services provided on industry structure and economic growth?
- What is the impact of the project, technology, application or services on the human rights of individuals, clients, users, employees and/or contractors?

Economic and financial impact

- What is the total cost of the system – in developing, deploying and maintaining the system?
- Has the organisation considered more cost-effective alternatives or whether the surveillance system is necessary at all?
- How will the cost-effectiveness of the surveillance system be measured?
- Will the government [or company] get value for money from the proposed surveillance system?
- Could the funds spent on developing, deploying and maintaining the system be used better in some other way?
- Does the surveillance system, e.g., social networks such as Facebook, exploit "free" labour (users contribute their personal data and time free of charge to the system owner)?
- Will parties affected by the system incur expense?
- Will third parties incur expense as a result of the system?

Political considerations

- How will the electorate or consumers view deployment of the surveillance system? Will they accept or reject it?
- If it is a covert system, how will the public react if news of its existence comes to light?
- Who has taken or will take the decision to deploy the system?
- To what extent have stakeholders been engaged in the decision-making process?

- How "fit for purpose" is the surveillance system?
- Does the technology "chill" freedom of speech and association (e.g., are "smart" CCTV cameras and/or microphones installed in public places able to eavesdrop on conversations of the public as distinct from specific suspects)?
- Who is being surveilled by whom and for what purpose?
- Will the project or technology enhance the power of some at the expense of others?
- Who will have access to the data gathered by a surveillance system and how will such data be used?
- Will it undermine the electorate's trust in their elected officials?
- Will the surveillance system support or undermine democracy?

Security

- Is a new technology or project being introduced to improve security (whose security and which form of security is actually being improved)?
- How can we know if the claims of the security proponents are valid?
- Will a perceived increase in security take precedence over other values such as privacy?
- Who determines if security should take precedence?

Legal issues

- Does the surveillance system comply with legislation?
- Does the surveillance system support law enforcement (e.g., CCTV cameras on the metro can help apprehend those who assault or rob other passengers)?
- Is law enforcement the principal purpose of the surveillance system?
- If the surveillance system is deployed, will the owner and/or operator provide those surveilled with a right of inspection of how their data or images are being used, stored, and secured (and for how long)?

- Will those surveilled have a right of redress if their data or images are being used improperly or for purposes other than those originally specified?

Respect for constitutional principles of the modern democratic State

- Is there transparency with regard to why the surveillance system is being deployed?
- Is someone accountable for the legitimacy and efficacy of the surveillance system?
- Is the extent of the surveillance proportional and necessary in a democratic society?

Reversal of the presumption of innocence (into a presumption of guilt)

- Are *all* citizens subject to surveillance?

Fair trial/due process

- Are measures detrimental to citizens taken on the sole basis of evidence gathered through the use of smart surveillance devices?[3]
- Will the citizen be able to access the information used to take a decision concerning him or her?[4] In a timely manner? Will the citizen need the help of a lawyer (or any pertinently qualified person) in order to gain access to the information?
- Will the citizen targeted by smart surveillance measures be able to understand *why* he or she was subject to them?[5]
- Does the citizen have the possibility to contest such measures?

[3] This question is inspired from OSHCR (Office of the United Nations High Commissioner for Human Rights), "Human Rights Indicators: A Guide to Measurement and Implementation", HR/PUB/12/5, United Nations, New York and Geneva, 2012, [p.98].

[4] Ibid.

[5] Ibid.

Respect of equality between citizens and absence of discrimination

- Is the surveillance used for differentiated treatment of citizens on the basis of protected grounds (e.g., ethnicity, gender)?
- Is the surveillance measure used for differentiated treatment of citizens likely to have any side effects of differentiating between them on the basis of protected grounds?
- Is the surveillance applied indistinctly, where different personal situations ought to be acknowledged?

Impacts on ethical principles

Surveillance systems or technologies may impact ethical principles such as the following:[6]

[6] Most definitions of the ethical principles mentioned in this section come from Wright, David and Emilio Mordini, "Privacy and Ethical Impact Assessment", in Wright, David and Paul de Hert (eds.), Privacy Impact Assessment, Springer, Dordrecht, 2012.

Autonomy

The principle of autonomy refers to the individual's capacity for self-determination or self-governance. It encompasses two essential conditions: liberty (independence from controlling influences) and agency (capacity of intentional action). According to Kant, it is exactly in the virtue of our autonomy that we are capable of morality (moral autonomy). One of the most common objections to the concept of autonomy is that it is never possible to have any complete form of independence from contingent external influences.

- Does the surveillance technology, application or system positively or negatively impact the autonomy of the individual?
- Does the surveillance system impose any constraints on individual decision-making?
- How can the negative impacts on autonomy be avoided or minimised?

Dignity

The concept of dignity refers to the inherent status of human beings that entitles them to respect. The idea is to treat human beings as they deserve to be treated solely because of their humanity. Even if dignity is protected by the most important international legal instruments as constituting the basis of all other human rights, its definition remains difficult and elusive, since this concept touches the deeper spheres of the human condition.

- Does the surveillance system or technology intrude upon the individual's dignity?
- Does it intrude upon the individual's physical and/or psychological integrity?
- How can the impact of the surveillance system or technology on dignity be avoided or minimised?

Informed consent

Informed consent refers to the idea that the individual's consent must be based on a clear understanding of the situation to which he or she is consenting. In order to give informed consent, the individual must have adequate reasoning capability and must be free from any constraints.

- Have individuals freely given their explicit informed consent to being monitored, tracked and/or targeted?

- Is the individual subjected to a decision which is solely based on the automated processing of data?

Trust

The notion of trust "entails a belief in another agent's goodwill or veracity, a belief which in some sense goes beyond available evidence" (Encyclopaedia of applied ethics, Academic Press, 1998). In more concrete terms, trust can be defined as the expectation that an individual (distinguished by specific positive characteristics) will perform actions aimed at producing positive results for the "trustor".

- Will the surveillance technology or system erode trust?
- Will groups or individuals believe they are not trusted by others, especially those who are in a stronger position of power?

Justice and fairness

The concept of justice is one of the most complex in ethics. In its narrower sense, the concept involves the idea of acting in accordance with the principles of fairness, equity, non-discrimination, i.e., those persons have to be treated equally in similar situations. Justice here is interpreted to include equity and fairness, non-discrimination, solidarity and benefit-sharing.

- Are some groups treated differently from others? For example, corporate crime and workplace safety may be less surveilled than street crime, even though corporate malpractice may have much greater impacts.
- Is a specific group particularly targeted by the surveillance?
- Is there a rationale behind different treatment?
- Does the project facilitate discrimination or social sorting?
- Who benefits or loses from the surveillance scheme?
- Are participants aware of the benefits that may derive from the surveillance system or technology?
- Do participants have access to these benefits?
- Are benefits shared with a larger community?
- Will the technology or system erode social solidarity?

Responsibility

Responsibility refers to the need to ensure that someone can be hold accountable for an action (e.g., in this specific case, for complying with the principles presented in the SIA).

- Who will be accountable for ensuring that a surveillance impact assessment is properly conducted?
- Who will be responsible if a surveillance system is found to be unduly intrusive?
- Is an independent review of the SIA foreseen?

Non maleficence (avoiding doing harm)

The principle of non-maleficence asserts an obligation not to inflict harms on others. In relation to ICT-related projects, this principle can be useful to assess its impacts in terms of safety, isolation or substitution of human contact, and discrimination or social sorting

- Will the surveillance system cause undue or unjustified harm to anyone (see also the section above on dignity and the section below on psychological impacts)?
- Is there any concrete risk for the well-being of the individual?
- Can the information processed be used to cause harm?
- Is there a risk that the technology may lead to greater isolation of the individual?
- Is there a risk that the technology is seen as stigmatising (see also section below on Justice)?

Assets, threats, vulnerabilities and consequences

Surveillance can have positive and negative impacts. The focus here is primarily on the risks and the potential negative impacts.

Examples of assets

This section provides examples of the assets of individuals, groups, society, organisations at risk from surveillance. Assets can be tangible and intangible. Both are considered here. Almost all of the examples here are primary assets, but some of the examples may also be secondary assets (as noted below).

Individual assets include:

- Material or physical assets
- Personal data
- Privacy
- Dignity
- Autonomy or free choice
- Reputation or image
- Individuality
- Self-esteem
- Life-chances (opportunities) or one's job and/or career (revenue-generating capacity)

Group assets

- Material possessions
- Solidarity

- Autonomy
- Reputation
- Self-esteem
- Identity
- Freedom of expression and ability to contribute to public debate
- Integrity
- Right to dissent

Societal assets

- Social cohesion
- Solidarity and inclusion
- Democratic traditions, including freedom of expression and ability to contribute to public debate
- Tolerance

Assets of the organisation under surveillance

Within this group are both government agencies and companies. We also distinguish between organisations that could be under surveillance and organisations that are developing, deploying or operating surveillance systems, applications or technologies.

Several of the bullet points below are applicable to both companies and government agencies. However, the last three bullets are more likely to apply to just companies.

- Reputation
- Freedom to operate without being monitored
- Self-esteem
- Revenue-generating capacity
- Human resources
- Procedures and processes (may also be a supporting asset)
- Infrastructures
- Freedom to collaborate with others (mergers, acquisitions, associations, etc.)
- Trade secrets, proprietary knowledge
- Competitive advantage.

Assets of organisations developing or operating surveillance systems

- Reputation
- Self-esteem
- Revenue-generating capacity
- Human resources
- Procedures and processes (may also be a supporting asset)
- Infrastructures
- Freedom to collaborate with others (mergers, acquisitions, associations, etc.)
- Trade secrets, proprietary knowledge
- Competitive advantage.

Examples of threats

Surveillance systems may pose

- Threats to the individual
- Threats to groups
- Threats to society
- Threats to organisations

Threats posed by surveillance systems and/or technologies originate from those developing, owning or operating surveillance systems or technologies. These could include:

	Surveillants (threat source)	**Purpose of surveillance**	**Examples of threats**
1	The police	• To apprehend wrong-doers, to pre-empt crimes • to curtail civil disobedience or undesirable behaviour	• Recording (via CCTV) one's actions, • Interception of communications • Collecting and storing an individual's DNA and/or other biometrics behaviour, movements

	Surveillants (threat source)	**Purpose of surveillance**	**Examples of threats**
2	Intelligence agencies	• To apprehend potential terrorists • To ensure national security • To monitor activity in other countries	• Interception of communications • Monitoring the individual's activity on the Web
3	Local authorities	• To monitor those who drive into and out of dense urban areas • To deal with more minor offences that fall within their competences (thus not only limited to driving but also other offences, e.g., dumping rubbish)	• Monitoring vehicles, recording licence plate data
4	Other government agencies	• To check that those claiming benefits are actually entitled to them	• Data matching
5	Companies operating surveillance systems	• To gather personal data in order to influence or otherwise manipulate consumer behaviour	• Aggregating data • Data analytics • Targeting advertising
6	Companies spying on other companies	• To gain access to IPR or other proprietary information	• Social engineering (subverting an employee of the target company) • Web analytics • Interception of communications • Deception

	Surveillants (threat source)	**Purpose of surveillance**	**Examples of threats**
7	Hackers who install or operate surveillance systems	• To harvest personal data in order to commit fraud or other theft • As a political act, to show the vulnerabilities of a system	• Botnets
8	Terrorists	• To subvert a target political system or country • To cause panic and fear in a population	• Espionage • Distributed denial or service attacks
9	Transport operators	• To apprehend those committing assaults or thefts • To facilitate travel and economise on staff by offering smart cards	• Capturing images of people for subsequent analysis • Use of RFID-embedded travel cards, especially when linked with credit card data, to compile a record of individual travel patterns.
10	Airport authorities	• To maximise security and to target potential customers with personalised advertising • To co-operate with (transnational) law enforcement agencies	• Capturing images of people. • Using body scanners which have been likened to a "strip search". • Data matching as people progress through an airport's shops.
11	Health authorities	• To monitor the spread of diseases	• Data analytics
12	Insurance companies	• To optimise the setting of premiums • To minimise their liability and maximise profits	• Data aggregation and analytics

	Surveillants (threat source)	Purpose of surveillance	Examples of threats
13	Political parties	• To influence voters	• Data aggregation and analytics

Examples of vulnerabilities

Individual vulnerabilities

- Lack of awareness of the surveillance system or the effects of surveillance
- Social standing
- Lack of ability to resist surveillance
- Lack of resilience in response to surveillance
- Susceptibility to manipulation
- Lack of education or resources
- Power imbalances
- Lack of redress mechanisms

Group vulnerabilities

- Openness and transparency of the group
- Lack of awareness (the group may not be aware that it is being profiled or surveilled)
- Structure of the group (loose coalition vs. tightly coupled group)
- Prejudices
- Lack of history
- Lack of protection
- Minority and/or vulnerable groups (e.g., immigrants, children, old people, disabled)
- Groups slightly outside the mainstream (e.g., controversial groups)

Societal vulnerabilities

- Openness and transparency
- Lack of traditions of resistance and/or resilience
- Centralised power
- Fearful society
- Lack of awareness with regard to specific surveillance impacts

Vulnerabilities of the surveilled organisation

- Inadequate security of sensitive data
- Weak management
- Lack of adequate expertise
- Lack of adequate organisational culture

Vulnerabilities of the surveillant organisation (i.e., the owner or operator of a surveillance system)

- Inadequate processes and procedures
- Weak management routines
- Personnel
- Physical environment
- Information system configuration
- Hardware, software or communications equipment
- Dependence on external parties

Examples of consequences

Surveillance systems, technologies and applications may have both intended and unintended consequences. The following are examples.

Individual consequences

- Loss of self-esteem
- Loss of freedom and autonomy
- Costs (e.g., paying higher charges resulting from social sorting)
- Loss of trust

- Theft (someone uses the surveillance system to steal from the individual)
- Damage to reputation
- Damage to image
- Damage to revenue-generating capacity
- Damage to creativity

Consequences for groups

- Damage to self-esteem
- Damage to freedom and autonomy
- Democratic deficit
- Reduction in ability to recruit new members
- Reduction in the ability to demonstrate publicly
- Loss of integrity of the group's message or intention
- Chilling effect
- Damage to revenue-generating capacity
- Disintegration of the group
- Damage to reputation and image

Societal consequences

- Reduction in pluralism
- Democratic deficit
- Lack of transparency
- Reduction in constitutional safeguards
- Increasing dysfunction
- Polarisation
- Centralisation of power
- Nihilism
- Permanent state of exception
- Chilling effect

- Limited choices
- Damage to reputation
- Damage to image
- Damage to autonomy
- Damage to the economy
- Damage to democracy

Consequences for surveilled organisations

- Investigation and repair time
- (Work)time lost
- Opportunity costs
- Health and safety
- Financial cost of specific skills to repair the damage
- Damage to image reputation and goodwill
- Chilling effect
- Theft of IPR or other resources (from cyber espionage)
- Loss of personnel and employee commitment and trust
- Damage to revenue-generating capacity

Consequences for the surveillant organisations (those developing or operating surveillance systems)

The consequences for the organisation developing or operating a surveillance system may depend on who the target of the surveillance system is and the extent of exposure or awareness of what the organisation is doing.

- Investigation and repair time
- (Work)time lost
- Opportunity lost
- Health and safety
- Financial cost of specific skills to repair the damage
- Damage to image, reputation and goodwill
- Loss of personnel and employee commitment and trust
- Financial costs of developing the surveillance system

How to assign values in the assessment exercise

What assessment is expected in the following table? Ask: "How do you judge the risk of ... on the following assets?"

Table 1: Template for assigning values (one table per identified risk)

Asset	Number of possibly affected people (a)	Severity of prejudicial effect (b)	Overall assessment a + b	Explanation
Privacy - trans-parency - ...				
Asset 2 (affected value)				
Asset 3				
...				

The small-scale SIA questionnaire

The purpose of an SIA is to identify, assess and overcome the risks a surveillance system or technology poses for privacy, as well as for other societal and ethical values.

Stakeholder involvement in this process will help to identify risks, propose solutions, and ensure that a wide range of expertise and views are taken into account.

The first part of this questionnaire includes questions related to the legal, social and ethical implications and risks of the proposed project. The second section asks you to complete a risk map, according to the risks identified. The third section of this questionnaire asks you to identify potential solutions.

Legal Compliance

The following set of questions is included in order to identify any privacy issues associated with the legal compliance of the project. They are based on the eight fundamental principles of the EU Data Protection Directive 95/46/EC.

Data Protection Principle	Question	Yes or No
Fair and lawful processing	Do you have a legitimate reason for collecting and processing data? Is data used only for the specified and legitimate purpose? Is there a principle of transparency in place to inform about the collection and use of their data? Is data handled only in ways that an individual would reasonably expect? Is all data collection and processing legally compliant?	NO = ethical issue

Data Protection Principle	Question	Yes or No
Processed for limited purposes	Is personal information processed in any way? Is information linked or linkable to identifiable individuals? Is any sensitive information collected? Is data collected without a clear purpose defined? Is data collected without clear communication to the data subject (i.e., those subject to the surveillance system or technology)? Is data processed for any purpose other than that specified publicly? Is the data collected processed in a further way that is not compatible with the legitimate purpose as specified at the time of the collection?	YES = privacy issue
Adequate, relevant and not excessive	Is data collected and processed beyond those that are considered proportionate and necessary? Are there other means available to achieve the goals of the surveillance system that are less intrusive than the proposed surveillance system? Could the collection and processing of data be minimised, i.e., reduced to only what is absolutely necessary?	YES = privacy issue
Accuracy	Is data collected and processed beyond those that are considered proportionate and necessary? Are there other means available to achieve the goals of the surveillance system that are less intrusive than the proposed surveillance system? Could the collection and processing of data be minimised, i.e., reduced to only what is absolutely necessary?	NO = privacy issue

Data Protection Principle	Question	Yes or No
Data retention	Is data retained without a set period of time for deletion? Will any data be retained without a justification for holding that data? Is data retained without clear communication to the data subject?	YES = privacy issue
Transfer	Will data be transferred to a country outside the European Economic Area (EEA)? Is there potential for the organisation receiving the data in a non-EEA country to contravene the adequacy requirements of the EU Data Protection Directive?	YES = privacy issue
Processed in accordance with an individual's rights	Is it difficult for the data subject to correct their personal information? Is there potential for the processing of personal information to cause the data subject harm or distress? Will the data processed be used for direct marketing purposes without the data subject's consent? Is the surveillance system or technology designed in such a way that decisions affecting the data subject will be taken automatically, i.e., by the system rather than by someone in the organisation?	YES = privacy issue

Data Protection Principle	Question	Yes or No
Secure storage	Is the organisation putting in place a "need to know" policy to limit the number of people who might have access to the personal data held? Has the organisation considered various measures to ensure the secure collection, processing and storage of the personal data (e.g., encryption of data, access control measures, both physical and electronic, system redundancy, etc.) If personal data is held by a third party on your behalf are you satisfied with the third party's measures to ensure the security of the data?	NO = privacy issue

Other types of privacy

The previous section identified risks in relation to data protection and informational privacy. The purpose of a SIA is also to identify risks that go beyond legal compliance. The next section introduces a set of questions to identify the potential risks of the project associated with other types of privacy.

Type of privacy	Question	Yes or No
Privacy of the person	Does the surveillance system or technology involve a search or monitoring of a person's body (e.g., body scanners at airports or implants)? Does the surveillance system involve taking a bodily fluid (blood, saliva, etc.) without the person's consent? Does the surveillance system or technology involve requirements for submission to biometric measurement (e.g., fingerprints, retinal scan, facial recognition, etc.)?	YES = privacy issue

Type of privacy	Question	Yes or No
Privacy of personal behaviour	Does the surveillance system or technology involve monitoring a person's behaviour (e.g., relating to sexual preferences and habits, political or trade union activities and religious practices)? Does the surveillance system or technology involve monitoring a person's behaviour or recording speech (e.g., at a demonstration or a football match or passing through a shop or airport)?	YES = privacy issue
Privacy of personal communi-cations	Does the surveillance system or technology involve intercepting a person's telephone calls or Skype calls or text messaging? Does the surveillance system or technology involve access to a person's e-mail or other communications?	YES = privacy issue
Privacy of location and space	Does the surveillance system or technology involve tracking an individual wherever he or she goes (e.g., monitoring his or her position or location via a mobile phone)? Does the technology involve tracking an individual as the individuals goes from one website to another on the Internet? Does the tracking of an individual allow a picture of the individual's movements to be constructed?	YES = privacy issue

Type of privacy	Question	Yes or No
Privacy of association or groups	Does the surveillance system involve monitoring some groups of people (e.g., ethnic or religious minorities, people attending a demonstration, spectators at a football match)? Could the surveillance system or technology be used to discriminate in favour of or against some groups of people (e.g., some people are offered better prices than others depending on their socio-economic standing or where they live)? Will some groups of people be monitored and their images recorded (e.g., those attending a demonstration or football match or going to a mosque)?	YES = privacy issue
Privacy of organisations	Are the structures or internal secrets of organisations revealed through surveillance? Will the surveillance system or technology be used to support industrial espionage? Is the action of the surveillance system likely to impact on the function of any organisation or its ability to achieve its goals? Is the surveillance of the organisation likely to be known to the public? Might this have a negative effect on public perception of that organisation?	YES = privacy issue
Anonymity	Does the system surveil someone who would not have been under surveillance previously? Does this surveillance remove the possibility of anonymity?	YES = privacy issue
Right to be left alone	Is the individual subject to such surveillance that possibilities to seclude him or herself are reduced? Does this surveillance occur to such an extent that areas which would normally have been the individual's sole domain (e.g., his or her home or car) are also under surveillance?	YES = privacy issue

Type of privacy	Question	Yes or No
Right to freedom of expression and communication	Does the system impact on the ability of groups or individuals to freely receive or impart information?	YES = privacy issue
Right to free development of individuality and identity	Does the surveillance system affect the development of individual identity? Does the system impose a change in individuals' identity?	YES = privacy issue
Right to freedom of thought and religion	Does the system affect the possibility to develop, or manifest, cultural or linguistic identity? Does the system seek to reveal individuals' thoughts, beliefs or religious identities?	YES = privacy issue

Societal impacts

The questions that follow ask you to think about the potential societal issues associated with the project.

Impact	Question	Yes or No
Societal	Does the surveillance in question have a negative impact on social cohesion or trust? Does the project, technology, application or service increase or decrease social affiliation or isolation? Are their other options available to achieve a given social objective (e.g., a reduction in violent crime or in benefits fraud)?	YES = societal issue

Impacts on ethical principles

The questions that follow ask you to think about the wider ethical issues associated with the project.

Impact	Question	Yes or No
Ethical	Is the dignity of the individual protected under the surveillance system? Have individuals freely given their explicit informed consent to being monitored, tracked and/or targeted? Is trust between those surveilled and the organisation undertaking the surveillance or between individuals or groups and the government maintained and protected under the surveillance technology or system? Are there clear lines of accountability? Who will be responsible if the surveillance system is found to be unduly intrusive?	NO = ethical issue

Identifying Risks

An important part of risk assessment is to determine who might be affected by the privacy or surveillance risk and how they might be harmed.

According to your answers to the questions contained in the tables above, please now insert any identified privacy issues in the table below. The aim of this step is to identify any risks related to each privacy issue. Please also include the identified social and ethical issues.

Privacy, social, ethical issue	Risk to individuals	Compliance risk	Risk to the organisation
...	...	...	...

The risk map

The next step is to conduct a preliminary risk assessment, identifying the likelihood of a certain event and its consequences. In the following risk map, please rank the risks you have identified in the previous sections. These risks should be ranked according to how *likely* they are to happen, and against the *severity* if the event were to happen. Severity in this context can also be understood as *impact* or *consequence*. This exercise can be conducted individually or in a group.

Please first score the *severity* of the risk. This should be scored on a scale from 1 to 4 according to the following criteria:

1. *Negligible*: Individuals, groups, organisations and society either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.). Very few people (organisations or groups) will be affected by the feared event.

2. *Limited*: Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.). Some people – perhaps some specific groups – will be affected, but not that many as a percentage of the population.

3. *Significant*: Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of state of health, etc.). A large number of people will be affected – not everybody, but still a large percentage of the population.

4. *Maximum*: Individuals may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.). The whole of society, effectively everyone, will be affected.

Please note that severity can be ranked according to individual categories: privacy and/or social and/or ethical issues, individuals, compliance, and/or the organisation. Please conduct this stage of the exercise as many times as relevant from the point of view from which you are operating.

As a next step, please score the *likelihood* of a certain event (risk) happening. This should be scored on a scale from 1 to 4 according to the following criteria:

1. *Negligible*: The event is unlikely.

2. *Limited*: The event is fairly unlikely.

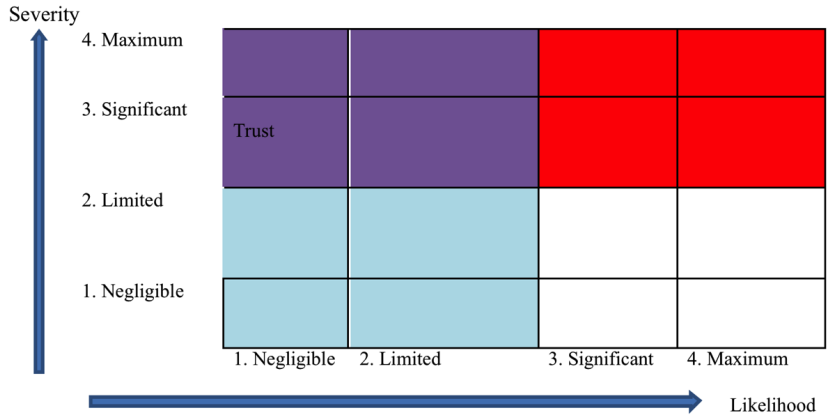
3. *Significant*: The event is fairly likely.

4. *Maximum*: The event is likely.

Please now plot your results on the risk map below. If you are conducting this exercise as an individual please fill in your scores directly. If you are conducting this exercise in a group, please add up

the scores for each category and divide by the number of people in the group to obtain the average. These average scores should then be filled into the risk map.

The example provided in the risk map below states that the proposed project eroding trust is unlikely (scoring 1), and that the severity in terms of impact would be significant (scoring 3).



Identifying solutions

In addition to identifying risks, the purpose of an SIA is to develop solutions to avoid, minimise, transfer or share risks associated with new surveillance systems or technologies. In the following table, please fill in any risk identified, as well as any potential solution that you feel is suitable to avoid, minimise, transfer or share that risk.

The example included is based on the risk identified previously and included in the risk map: the surveillance system or technology has the potential to erode trust.

Risk	Solution(s)	Result (is the risk avoided, reduced, minimised or transferred?)
Erosion of trust	Transparency: informed consent, effective communication of purposes of data collection/processing/transfer to the data subject	Minimised or possibly avoided
...	...	...

Co-ordinator:
Dr. Michael Friedewald
Fraunhofer Institute for Systems and Innovation Research ISI
Breslauer Straße 48 | 76139 Karlsruhe | Germany
Phone: +49 721 6809-146 | Fax+49 721 6809-315
michael.friedewald@isi.fraunhofer.de

Fraunhofer ISI

SAPIENT
Surveillance, Privacy & Ethics