EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CYBERSECURITY CERTIFICATION MARKET STUDY

Towards a research and analysis methodology

APRIL 2021

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. For more information, visit www.enisa.europa.eu.

CONTACT

For contacting the authors please use certification@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

CONTRIBUTORS

ECORYS Nederland BV, The Hague Centre for Strategic Studies.

EDITORS

Prokopios Drogkaris, European Union Agency for Cybersecurity.

ACKNOWLEDGEMENTS

We would like to thank the members of the ENISA NLOs Network for their valuable comments and insights.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN: 978-92-9204-500-5 - DOI: 10.2824/919706

EXECUTIVE SUMMARY

Drawing up EU cybersecurity certification schemes aims at providing harmonised criteria to carry out conformity assessments to demonstrate the degree of adherence of ICT products, ICT services or ICT processes against specific predefined cybersecurity requirements. From an economic perspective, these evaluations might subsequently also address imbalances in the market that could lead to suboptimal outcomes. Cybersecurity certification also touches upon socio-economic aspects such as user trust and market responsibility of the owner of the certificate. Further to that it also touches upon the need to provide a reasonable level of cybersecurity for a 'duty of care' throughout the ICT product, ICT service or ICT process lifecycle and the prevention of costs of a cybersecurity failure and subsequent loss of market reputation. Therefore, the drivers for cybersecurity certification in the EU go beyond cybersecurity requirements.

This study proposes a set of initial methodological steps to work towards a market analysis on cybersecurity certification of ICT products, ICT services and ICT processes. The performance of a market analysis on cybersecurity certification aims to contribute to the EU cybersecurity certification framework and the planning activities of the European Commission, the ECCG and the SCCG by identifying future areas for cybersecurity certification.

The proposed steps described in this study are divided into four main sections and cover:

i) the identification of the context of the market analysis,
ii) the scope of the target of analysis,
iii) assessing the impact of a cybersecurity certification initiative and
iv) the identification of the available options and possible initiatives.

The goal is to be able to identify certification needs or 'gaps' in the market without relying solely on input of stakeholders, but rather to provide evidence both from the supply and demand sides while factoring societal and economic aspects.

This first attempt on proposing such a methodology is expected to evolve and to be further developed and improved after the publication of the Union Rolling Work Programme by the European Commission. It is expected that a more mature market analysis methodology will be able to generate information that feeds the identification of the strategic priorities set by the European Commission, the ECCG and the SCCG. The methodology also aims to provide valuable input to the preparations of candidate cybersecurity certification schemes.

TABLE OF CONTENTS

1. INTRODUCTION

The EU cybersecurity certification framework, established under the Cybersecurity Act (CSA)[1], is an instrument that aims to establish and maintain trust and security in Information and Communications Technology (ICT) products, ICT services and ICT processes. Drawing up cybersecurity certification schemes at EU level aims at providing harmonised criteria to carry out conformity assessments to establish the degree of adherence of the products, services and processes against specific predefined requirements. The Union Rolling Work Programme (URWP) is a strategic document that allows industry stakeholders, Member States and standardisation bodies to get a clear view on future EU cybersecurity certification schemes. It is a multiannual overview of future candidate schemes and provides a midterm overview of the defined future fields of certification, which the European Commission intends to submit to ENISA. The URWP is drafted in close collaboration with the European Cybersecurity Certification Group (the 'ECCG') and the Stakeholders Cybersecurity Certification Group (the 'SCCG').

EU cybersecurity certification schemes are expected to touch upon socio-economic aspects such as user trust.

EU cybersecurity certification schemes will primarily address the level of cybersecurity required for ICT products, ICT services or ICT processes. From an economic perspective, they could address imbalances in the market that lead to suboptimal outcomes and could also touch upon socio-economic aspects such as user trust, the duty of care of a manufacturer or provider and prevention of cybersecurity failure to protect market reputation. Therefore, the drivers for cybersecurity certification in the EU go beyond cybersecurity requirements. This broader understanding and oversight would be beneficial to the policy and regulatory certification activities of the European Commission.

Towards this direction, ENISA, conducted as part of its Annual Programming document 2020 (under Output O.5.1.2) a study on identifying a set of methodological steps to allow for a market analysis on cybersecurity certification of ICT products, ICT services and ICT processes. While preparing these steps, the following considerations were taken into account:

1. **How to segment the cybersecurity market and what is the "Target of Analysis":** Analysing the cybersecurity market is complicated looking at the number of security vectors for ICT products, ICT processes and ICT services as well as the complex nature of the supply chains and complex systems with a lot of ICT components. For example, Connected and Automated Mobility (CAM) have numerous security vectors: technical, processes, and principles. At the same time, they include complex structures of components and create a multipart supply chain. Within this supply chain there are also segments of analysis including sensors, smart devices/ Internet of Things (IoT) devices, cloud computing, Industrial Automated Control Systems (IACS) and other areas. Disentangling these levels for analysis is a crucial first step to conduct a market analysis. Lastly, introducing cybersecurity solutions in one area may have knock-on effects in other sectors of the economy, which also need to be taken into account.
2. **How does the reasoning of the request influence the market analysis:** There are two basic reasons to conduct a market analysis: i) to determine whether an cybersecurity certification based intervention is required, especially in an emerging market or ii) to determine the performance of a new security scheme and whether it is improving market performance. If the analysis is being conducted to understand

[1] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) http://data.europa.eu/eli/reg/2019/881/oj

market performance, the methodology addresses issues related to cybersecurity requirements, trust building or how it could help to address societal challenges.

1.1 SCOPE - OBJECTIVES

The objective of this study is to propose a set of methodological steps to allow for a market analysis on cybersecurity certification of ICT products, ICT services and ICT processes. It attempts to strike a balance, providing a list of steps and potential questions that can be asked without creating a textbook on how to conduct particular types of economic analyses. It provides a methodological toolbox that can be applied to the cybersecurity market. This toolbox includes caveats about the use and limitations of individual tools, their combinations, what types of conclusions can be reached with their help and what needs to be considered when interpreting the results. Further to that, it incorporates potential costs (e.g. man/days and cost of data purchase) associated with the use of the toolbox, whether there are interdependencies with other activities and/or stakeholders and what quality assurance measures will be necessary to produce better results.

1.2 STRUCTURE OF THE DOCUMENT

Chapter 2 of the study provides further context on the questions to ask before conducting a market analysis, including understanding how to best scope the market of interest and how to develop specific research questions that the market analysis is looking to answer. Chapters 3 and 4 provide step-by-step approach that can be used to guide a market analysis, providing a set of indicative questions that could be used. Lastly, Chapter 5 concludes the study and provides indications of how it could support the activities of the European Commission, ENISA, ECCG and the ECCG. At the end of this report, a set of annexes provide indicative guidance for specific aspects of market elements.

2. CONSIDERATIONS PRIOR TO THE ANALYSIS

2.1 SCOPING AND SEGMENTATIONS OF THE CYBERSECURITY MARKET

Market segmentation is usually used to assess individual parts of a specific market[2], providing scope and boundaries to any analysis of relevant trends, evolution and performance. These boundaries will be vital, depending on the scope of each analysis, because without clear borders, a market analysis can quickly devolve into a massive exercise that touches on more cybersecurity aspects than those really needed in the economy. For example, if an analysis aims to cover Connected and Automated Mobility (CAM)[3], it potentially includes[4]:

- **Connected services and off-board systems** that are characterised by agile development cycles involving the continuous evolution of services following staggered releases; a large number of short-term projects generally based on scalable and modular cloud architectures.
- **Various physical infrastructures, equipment, products and associated services, vehicles and soft-mobility devices** based on Operational Technology (OT), electrics/electronics (E/E) architectures which must meet the security and technical requirements associated with various types of quality validations or regulatory approvals (e.g. vehicle type approval).
- **Wireless networks,** including automated guided vehicles (AVGs) and human interface systems (HMI) as equipment. Products and associated services are connected by, for example, Bluetooth, Wi-FI/WLAN or other wireless techniques.

Such a scoping exercise is particularly necessary as policy-makers tend to have broader socio-economic interests compared to a market analysis designed for private-sector entities, where questions around the market are narrower in focus. A market analysis within the context of cybersecurity initiatives needs to take into account the interests of (end) users, stakeholders, employees, policymakers, and national authorities as well. Segmentation can take place along a number of different aspects which include among others:

- type of ICT product, ICT service or ICT process;
- application area;
- sector;
- stakeholders involved and/or concerned;
- technologies used and or deployed;
- geographical boundaries of the market.

The final selection of the segmentation—the target of analysis—will depend largely on the research questions that the activity is looking to answer. Criteria by which the target can be scoped are determined by a number of factors, including:

[2] Dolnicar S., Grün B., Leisch F. (2018) Market Segmentation Analysis. In: Market Segmentation Analysis. Management for Professionals. Springer, Singapore. https://doi.org/10.1007/978-981-10-8818-6_2
[3] Connected and automated mobility in Europe. European Commission. Retrieved from: https://ec.europa.eu/digital-single-market/en/connected-and-automated-mobility-europe#
[4] ENISA, 2020, Cybersecurity Stocktaking in the Connected and Automated Mobility (CAM) https://www.enisa.europa.eu/publications/cybersecurity-stocktaking-in-the-cam

1. **The market needs that the analysis wishes to (potentially) address.** This first criterion can be a “chicken and egg” situation. One of the reasons to conduct a market analysis is to understand areas where a market is not functioning in an optimal way. At the same time, a market will generally only become of interest when stakeholders are raising particular issues, or when innovative developments in technology seem promising, which generally means that there is at least some starting point for why the analysis is being conducted.
2. **The data available for the study.** Available data on market size, market shares, value chains, revenues, market consumers and other relevant elements will be key to providing the quantitative basis for a market analysis, and the more datasets that are available, the easier an analysis becomes. As discussed in the following chapters, datasets in high-tech -particularly for new technologies - can be quite difficult to reveal or find (or may be of dubious quality).

Ideally, the source of information on how to segment a market and determine the final target of analysis should come from available expert market knowledge, but for ‘undefined’ markets, this may not be at hand. Under these circumstances, it will be necessary to seek out views from various stakeholders. Stakeholders that may be consulted to help determine the scope are indicatively listed below:

- **Industry experts from business associations**: Business associations will have direct links to the companies affected by cybersecurity issues, and they will have a broad access to useful insights. Being associations they will also be able to provide an overview of issues across a sector.
- **Industry experts from business consultants**: Industry experts and business consultants will come from multiple perspectives. They will tend to have a broad overview of a sector, and they may also have more insight into the operational elements.
- **Private Sector company experts**: Companies will be able to provide direct information on the costs to their business and will already have a good understanding and prior experience with market analyses.
- **Small and medium-sized enterprises (SMEs) and start-ups:** Getting direct access to SMEs is an ideal data source as they will have the same insights into business operations as larger operations, but will have experience on how to better access a specific market and how to meet its needs. Start-ups often have a good view on new markets to explore and are able to provide trendsetting information.
- **Consumers and consumer associations:** Consumers can provide the requirements and needs from the end user perspective and highlight the societal and possible acceptance aspects and their needs.
- **Regulators and policymakers:** Regulators and policymakers, particularly those responsible for regulating a specific sector or policy area, will have insights into both how the sector works, as well as in relation to other sectors and look into the broader socio-economic impacts - both positive and negative - of activities within a particular sector.
- **Researchers and academia:** Academics will have a broad overview of the sector from numerous perspectives. They are the most likely to provide research information on possible market developments, or opportunities or information related to the effectiveness of (new) analysis methods. They may answer questions in an unprejudiced manner and can also highlight recent research results.

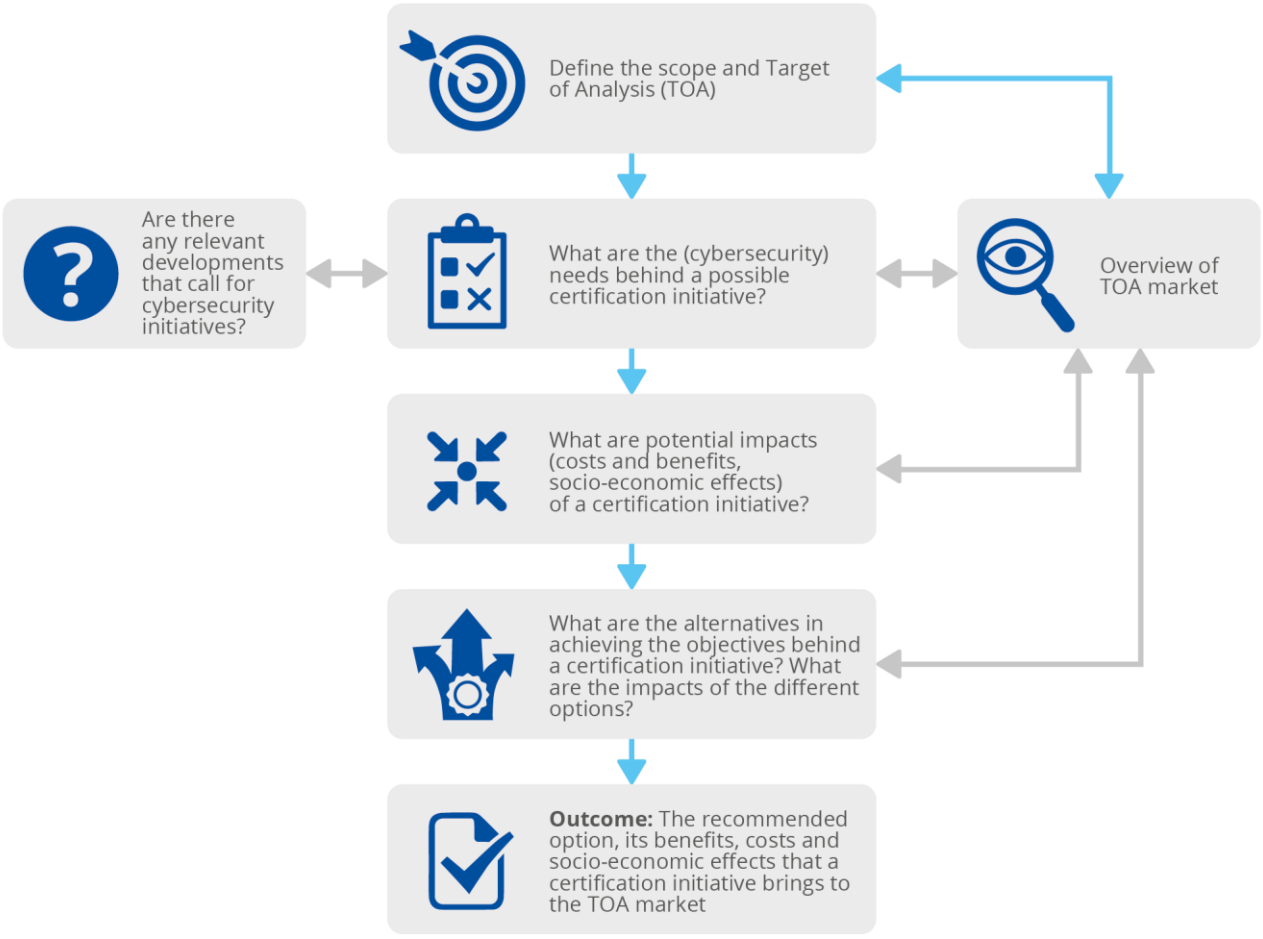
2.2 DEVELOPING RESEARCH QUESTIONS

While there are typical methodologies and research questions that need to be asked, as outlined in the steps that follow in this study, a market analysis can be guided by broader research questions. Taking the IoT market as an example; is the primary reason to analyse the market because of the well-known cybersecurity incidents or risks for companies to adopt business models that provide better cybersecurity over the long-term? Or rather, is the primary reason to analyse the market and understand whether advertised security failures are a barrier to further uptake? Developing broad research questions will allow us to provide a broader context to a study being conducted and also determine what resources will be focussed on when a market analysis is being conducted.

3. PROPOSED WORKFLOW

The following two chapters provide the workflow for how to conduct an assessment of the Target of Analysis (TOA). While the steps indicated in the diagram below are described as sequential, it is possible that at a certain moment either the TOA or the scope of a certification initiative needs to be adjusted. Therefore, there are potential iterations between the steps. The following diagram provides an overview of the overall workflow in brief, which is further detailed in Chapter 4.

Figure 1: Workflow for how to conduct an assessment of the Target of Analysis (TOA)



Within this workflow, further described in the following chapter, there will be two main types of analysis:

- **Market assessment:** A market analysis will be conducted in a market segment where there is currently no EU cybersecurity certification initiative. This type of market analysis aims to determine whether there is a justification for EU to consider new initiatives to be developed, to identify the focus of possible new initiatives or to confirm the scope of a future initiative.

- **Impact assessment:** A market analysis could support the activities of the EU cybersecurity certification framework on reviewing the effects of EU cybersecurity certification. In this case, the scope of the TOA should be easier to determine, because it will be determined by the effects a scheme has on the market, given its scope that is the focus of the analysis.

The following Chapter provides a set of methodological steps and a series of questions that need to be answered at each stage of one of these two types of market analysis. In addition to the questions to be answered, each step lists the envisioned output that should come from the analysis as well as the methodologies that could be applied.

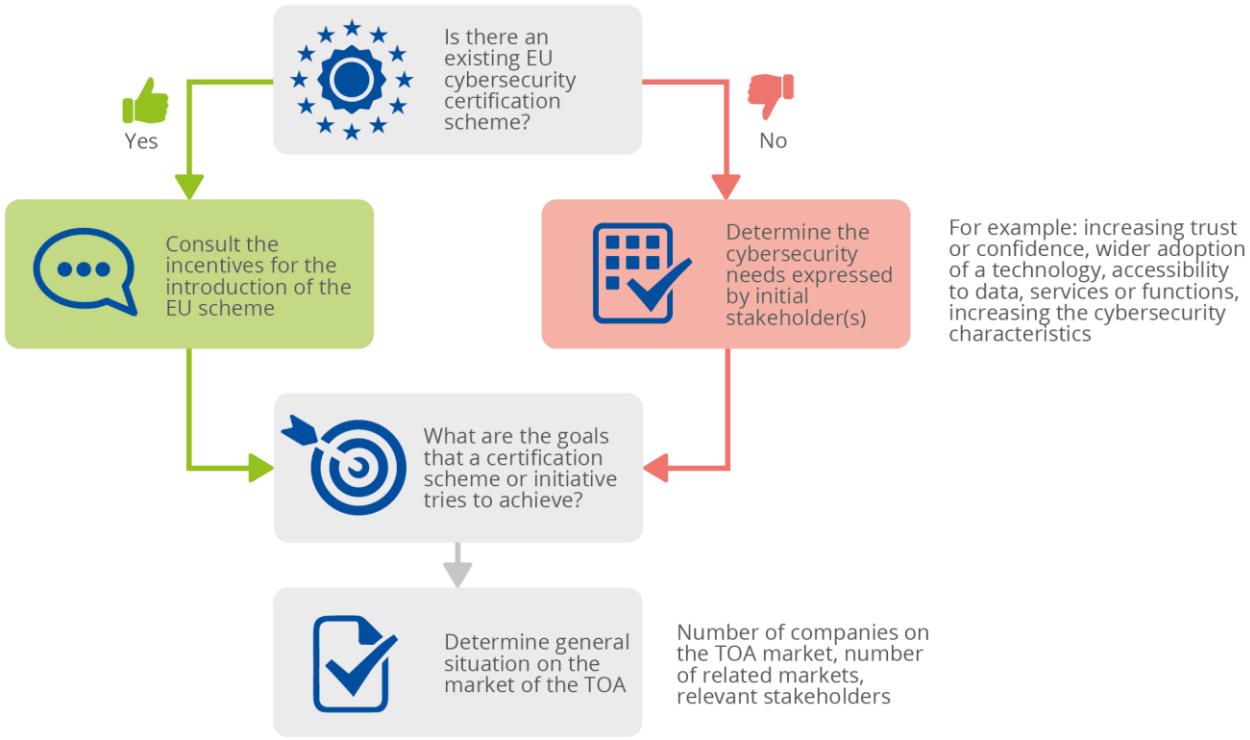
4. PROPOSED METHODOLOGICAL STEPS

4.1 STEP 1: DETERMINE THE CONTEXT AND THE SCOPE OF THE TOA

The goal of this step is to determine the context and the scope of the TOA, by answering the following questions.

- What are the cybersecurity considerations or relevant developments that demand cybersecurity initiatives on the 'market' of the TOA?
- What considerations should a cybersecurity certification initiative address?
- Who would be affected/involved?

Figure 2: A schematic representation of this step is provided below in addition to the relevant questions.



Q.1	Is there an existing EU cybersecurity certification scheme for the TOA? - If yes, conduct **"impact assessment"** - If no, conduct **"market assessment"**
Q.2	Does the market analysis relate to a specific sector or application area?
Q.3	How many (potential) producers/manufacturers exist on the market of TOA?
Q.4	Who are the (end) users operating, involved or affected by the TOA? - Individual consumers/end users - Suppliers of intermediary input (process, product, service) for the TOA - Government/public organisations - Regulatory organisations/bodies - Private sector organizations
Q.5	Will changes imposed on the market of the TOA have an impact on other markets? - If yes, which markets other than the TOA markets?
Q.6	How many and which industry verticals does the TOA influence?
Q.7	How many subordinate ICT products, ICT process or ICT services does the TOA depend upon?
Q.8	Do cybersecurity initiative(s), such as voluntary certification schemes, standards, technical specifications and/or guidance, exist for the TOA? - If yes, what is the geographical coverage and acceptance so far?
Q.9	Does the lack of an EU cybersecurity certification scheme for the TOA contribute to higher direct macroeconomic costs (due to verification and insurance costs, higher rates of litigation and/or product/service failure)?
Q.10	Does the lack of an EU cybersecurity certification scheme for the TOA contribute to higher indirect macroeconomic costs (due to inhibited market growth, societal unease due to uncertainty of application, lack of international coherence, fragmentation of the cybersecurity market and incoherence between vertical and horizontal markets, etc)?

Consultation of experts via interviews or surveys shall contain the questions listed above. Different aspects of the TOA, from the composition of the market to the availability of different cybersecurity initiatives, assessments of the cybersecurity for the TOA, could be retrieved from existing literature when attempting to answer the questions listed above. This may provide a more complete overview.

4.2 STEP 2: PRELIMINARY ASSESSMENT OF THE IMPACT OF A CERTIFICATION INITIATIVE

The goal of this step is to assess preliminary how a cybersecurity initiative impact/will impact the market of the TOA, by answering the following questions:

Q.11a	If "**market assessment**", assume you could create a certification initiative for the TOA. - What should be achieved by acting at EU level? - Which costs and benefits do you anticipate to have and which stakeholder groups will be affected?

Q.11b	If "**impact assessment**", which costs and benefits occurred/were accrued on the market for the TOA after the launch of a certification initiative?

Table 1 below includes an indicative but not exhaustive range of various costs that are typically incurred by the stakeholder groups such as businesses, government/public authorities and citizens.

Table 1: Costs that might be associated with a potential cybersecurity initiative

Cost type	Sub-category
Direct costs	Administrative costs
	Charges, Fees etc
	Other compliance costs
	Administration and enforcement
Indirect costs	Costs incurred in related markets or experienced by actors that are not directly targeted by the certification
	Indirect compliance costs
	Negative market impacts (such as Reduced market access)

Table 2: Benefits that might be associated with a potential cybersecurity initiative

Benefit type	Sub-category	Short description	Who potentially benefits?
Improved market efficiency	Sub-categories are the same as the classification for costs	Improved allocation of resources, removal of regulatory or market failures or cost savings generated by (new) certification scheme. It could also result in reduced prices for end users.	• The whole economy

Benefit type	Sub-category	Short description	Who potentially benefits?
	Increase willingness to pay for a certified product	Enhanced reputation of businesses producing the certified product/service/process, and thus increased trust of consumers	• Businesses producing/selling the certified product/service/process
Indirect compliance benefits: Spill-over effects related to third party compliance with a certification scheme			• Businesses in related markets • Individuals/customers in related markets
Indirect wider macroeconomic benefits		An increase in GDP, improved competitiveness; improved productivity	• The whole economy
Other wider society benefits		Increased protection of fundamental rights, social cohesion, international stability; Enhanced cyber security	• The whole economy

After answering the questions on the potential costs and benefits associated with a (potential) certification initiative, consider the following:

Q.12	What data sources would you need to consult to quantify and identify the financial and socio-economic costs and benefits?

Data sources and data collection methods could include: usage of secondary sources (desk research), Interviews and survey, Delphi method[5] with either potentially affected stakeholders or experts in the market of the TOA, consulting subject matter experts, etc.

Q.13	Is it realistic to quantify (in financial and socio-economic values or qualitatively)? - If yes, continue quantifying. - If no, go back to step 1, and consider the form that a cybersecurity initiative might be taking. If the scope of a cybersecurity initiative is quite narrow, continue quantifying. If it is not realistic to quantify, go back to step 1 and narrow down/scope the TOA in more detail (this also results in an adjusted output of step 1). - Is it realistic to quantify the financial and socio-economic costs and benefits given the adjusted description and scope of the market of the TOA? - If you continue saying no to (c), repeat (b), until you're able to respond yes to (c).

[5] https://www.rand.org/topics/delphi-method.html

Once you analysed the financial and socio-economic costs and benefits, you may consider checking them by answering the following questions:

- What goals does a cybersecurity initiative attempt to achieve?
- Could alternative solutions be imposed to achieve the goals pursued?
- Are the methods used for the assessment of financial and socio-economic costs and benefits satisfactory?
- Are any financial and socio-economic costs or benefits omitted?
- Are the methods used providing a reliable evidence?
- Does the assessment of financial and socio-economic costs and benefits allow for uncertainty in them? Could the change in the assumptions affect the estimated financial and socio-economic costs and benefits? If yes, how it would affect them and why?
- If you can make a decision to introduce a new cybersecurity initiative, what would the recommendation be?

4.3 STEP 3: IDENTIFY AVAILABLE OPTIONS

The goal of this step is to determine options of acting at EU level, by answering the following questions: What are the various options? At what level (national, EU and international) could they be taken? What form could various options (regulatory and non-regulatory means) take?

More specifically, the following questions need to be answered:

Q.14a	If "**market assessment**", determine options or forms of a new scheme: - Developing a completely new scheme; - Endorsing an existing one and developing one based on it; - An option for comparison is also a situation where no new scheme is created.

Q.14b	If "**impact assessment**", a comparison point is the counterfactual or a situation that could have happened in case a certification scheme was not created and not imposed.

Similar to the previous step, a number of questions could be considered for appraising the calculated costs and benefits of different options:

- Are the identified goals of the cybersecurity initiatives given the financial and socio-economic costs and benefits possible to achieve?
- Are other options possible looking at the alternative solutions that could be imposed to achieve the goals pursued?
- Are the methods used for the assessment of financial and socio-economic costs and benefits effective for the solutions?
- Do the methods used provide a reliable evidence? Does the assessment of financial and socio-economic costs and benefits allow for uncertainty in them? Could the change in the assumptions affect the estimated costs and benefits? If yes, how it would affect them and why?

4.4 STEP 4: COMPARE THE IMPACT OF POSSIBLE OPTIONS

The goal of this step is to compare the differences in impacts of various options, by answering the following questions

- What are the impacts of the (financial and socio-economic) costs and benefits of the different policy options?
- What are the differences and who will be affected by them?
- How do the objectives/goals of the different options relate to each other, looking at their reachability/pursuance at EU level?
- Compare the options and prioritise the level of realistic achievements
- How do the different options compare in total?

Q.15a	If "**market assessment**", compare the market results of the financial and socio-economic costs and benefits of the different options.

Q.15b	If "**impact assessment**", compare the impact of the financial and socio-economic costs and benefits of the current situation (with an existing certification scheme) to a counterfactual (situation without a certification scheme)

Q.16	If the differences between financial and socio-economic costs and benefits cannot be quantified, go back to step 3: determine options for comparison, and redefine the options to narrow it down; then continue with comparison.

Q.17	If you still cannot quantify the differences between financial and socio-economic costs and benefits, go back to Step 1 and narrow down the scope of the market; then repeat Q.13 or Q.14 and Q.11 or 12 until you're able to quantify the differences in financial and socio-economic costs and benefits.

4.5 STEP 5: SELECT THE OPTIMAL OPTION

Q.18	Which option is expected to yield the highest net benefits?

Similar to the previous step, a number of questions could be considered for appraising the calculated (financial and socio-economic) costs and benefits of different options:

- Why does the best option fit the goals in the most optimal way?
- Why are the methods used for the assessment of financial and socio-economic costs and benefits most satisfactory in terms of reliability and adaption flexibility in assumptions?

5. CONCLUSIONS AND NEXT STEPS

One of the main objectives of the EU cybersecurity certification framework is to increase trust and the cybersecurity reliability of the in ICT products, ICT services and ICT processes and to address the needs of the EU cybersecurity market. This study aims to provide a set of methodological steps to identify, gather, analyze and understand these needs. They can relate to emerging cybersecurity certification needs but also to existing certification schemes under the CSA. It aims to support an analysis on how schemes are adopted by the market, at defined moments, and if further adaptations are needed by the involved stakeholders. Analysing the cybersecurity market is complex due to the number of security vectors or ICT products, ICT processes and ICT services, as well as the complex nature of supply chains that become larger due to increasing connectivity and the number of components that may be part of large systems.

This proposed set of methodological steps attempts to create a structured and step-by-step approach to identity cybersecurity needs in a complex environment. It aims to provide a practical guidance to analyse the market, without though creating a textbook on how to conduct particular types of economic analyses. These proposed steps are divided into four parts and cover the identification of the context of the market analysis and the scope of the target of analysis, assessing the impact of a cybersecurity certification initiative, identification of the available options and possible initiatives. The goal is to be able to identify gaps in the market - from a cybersecurity certification perspective - without relying solely on input of stakeholders, but to provide evidence both from the supply and demand sides while factoring societal and economic aspects.

This first attempt on proposing such a methodology is expected to be further developed after the publication of the Union Rolling Work Programme by the European Commission. It is expected that in a more mature state, a market methodology will be able to provide valuable input for the identification of strategic priorities by the European Commission, the SCCG and the ECCG, even for future editions of the Union Rolling Work Programme. In addition, it may also support ENISA in maintaining the EU Cybersecurity Certification Framework, and provide input for the preparation of future candidate cybersecurity certification schemes, even outside the Union Rolling Work Programme, upon request of the European Commission or the ECCG.

A ANNEX: HOW TO ASSESS THE COSTS AND BENEFITS OF A CERTIFICATION INITIATIVE

Different methodologies could be used to estimate potential costs and benefits due to a certification initiative. The choice of a method depends on several factors:

Consideration	Description
The scope of a certification scheme	When different types of costs can be broken down to a relatively precise set of activities to be carried out, the costs are more easily estimated adding up the various costs of these activities for a type of relevant (impacted) stakeholder. A more qualitative approach could be more suitable in a situation when a complex certification scheme is considered, where a range of starting positions across affected (and regulated by the cybersecurity initiative) entities is wide and/or there are potentially numerous ways in which stakeholders are impacted.
The expected compliance costs and the expected resources to be dedicated	The higher the expected costs (in particular the compliance costs) or the wider the scope of the certification initiative (or the number of different options for comparing different certification schemes), the higher the amount of resources needs to be invested in estimating the costs and benefits.
The availability of data	The greater the availability of data, the more costs and benefits could be quantitatively estimated.
Assumptions about costs and benefits	Assumptions might affect the magnitude and size of the impact. Therefore a check should be performed on how a change in assumptions affects the costs and benefits.

The costs and benefits can be quantified through estimates based on financial, economic and statistical data gathered from various sources through:

- Determining costs and benefits from secondary sources (desk research)
- Interviews
- Survey
- Delphi method
- Modelling.

Annex D presents a table overview of different methods with their advantages, limitations and potential risks.

A monetary value could be assigned to direct costs and other tangible costs (administrative costs) and benefits. For other types of costs and benefits it could be difficult to assign a monetary value. Instead, it could be assessed qualitatively. Most likely, the costs depend on a specific form that a certification initiative takes, while benefits are most likely to be similar

between different types of initiatives. If it is the case, then only costs of different forms of initiatives could be assessed and compared.

The costs and benefits are to be compared over time. Therefore a discount rate could be included in the calculation. In case different options of a cybersecurity certification initiative concern the same timing, the assumptions about a discount rate are less relevant. On the other hand, when costs and benefits are incurred at different times, it is necessary to apply such a rate to compare them on an equivalent basis. The need for assigning a discount rate arises from the fact that the value of one euro paid today is greater than the value of one euro paid at some point in the future.

It is possible that a certification initiative might result in some distribution of a welfare between businesses, consumers, or other players. It is therefore very important to assign which benefits and costs are relevant for each type of stakeholders on the market of the Target of Analysis (TOA).

A preliminary assessment of costs and benefits of a potential cybersecurity initiative can provide a general indication of the scale of the costs and benefits likely to be imposed. A qualitative assessment could be performed to rank the costs and benefits into low, moderate or high/major in size. This helps to identify the major cost drivers of a cybersecurity initiative and might result in reformulation of what the initiative might entail.

When specific data in question is not available, benchmark figures or rules of thumb could be used. These are for example economy-wide average wage figures, instead of specific estimates derived from industry of the likely wage costs and benchmark figures for overhead expenses.

Economy-wide averages for the estimation of costs and benefits
Data is available for the EU-27 in Eurostat on a range of indicators such as wage costs and real added value; however, such averages calculated for the EU-27 most likely do not reflect the costs in a specific sector that is not defined as part of NACE Rev 2 sectors or industries.

A.1 NUMBER OF AFFECTED STAKEHOLDERS

Determining the size of the group that would be subject to a proposed cybersecurity initiative is crucial to developing reliable estimates. The risk of making large errors in estimating these numbers is often likely to be much greater than the risk of similarly large errors in estimating the unit costs to individual businesses or regulated parties of complying with particular regulatory requirements. This means that research on the number of affected parties should generally receive high priority. When a cybersecurity initiative concerns a specific industry or industries, potential sources of information on which to base estimates of the number of affected firms include:

- governmental statistical offices, for example, Eurostat;
- industry associations;
- academic research;
- licensing or registration data if available;
- information from regulators in other, comparable jurisdictions;
- surveys of potentially affected industry sectors (either existing survey-based data or the results of surveys undertaken as part of the costs and benefits assessment process).

If an initiative focuses on specific areas rather than affects a wide population, generally available information from government statistical source is less likely to provide relevant guidance. Consultation with industry associations or other representative bodies may provide usable data, particularly where these bodies have a large membership, covering a significant proportion of the affected group.

Surveys may be expensive and time consuming to conduct both for government and for stakeholders. Therefore they may not be feasible to perform. However they could be justified if expected impacts are significant. Small-scale surveys or Delphi method can provide broad indications of the scale of expected impacts and feedback could be gathered on the magnitude of the costs and benefits.

A.2 QUANTIFYING THE COSTS

The costs could be direct and indirect. The direct costs are those borne by the businesses targeted by the cybersecurity initiative and authorities. The indirect costs are less tangible and could be borne by those not targeted by the cybersecurity initiative.

The direct costs could be one-off or recurring costs. Therefore making a decision on the frequency of costs will impact the quantification of the costs. It is included in each type of costs quantification as frequency. The relevant costs parameters could be identified through the table and the checklist of costs and benefits that could be associated with a certification initiative. In case some costs are incurred in a situation “business as usual”, then those shall be subtracted from the costs associated with a certification initiative.

The “business-as-usual” costs are usually assumptions about:

- the costs that would not be avoided if a cybersecurity initiative were to be repealed in case a cybersecurity initiative already exist; or
- the costs that are already borne by various parties that will continue to bear these costs if a new cybersecurity initiative is imposed.

The “business-as-usual” costs are often obtained by consulting targeted stakeholders or experts. Since these costs are not a result of a newly imposed cybersecurity initiative, it could be easier to simply mark which costs are “business-as-usual” and which ones are directly associated with the cybersecurity initiative. In case it is not possible to do so, such costs could be estimated by looking at the share of costs associated with a substantive obligation that are borne by similar entities that are not targeted by specific legislative provisions: when this is the case, you can observe the level of compliance costs for the “regulated” entities and the “unregulated” ones, and take the difference as the relevant portion of costs to be considered in your estimate.

All costs might be different over the life of the (proposed) cybersecurity initiative (not considering the discount factor). If it is the case, such differences need to be accounted in the calculation. In principle the costs are a multiplication of the amount of time spent on a specific action to comply with the requirements of a cybersecurity initiative (list of specific actions associated could be used from Annex B) and the salary costs for the actors performing the actions. The sub-sections below provide an initial indication of how these costs can be quantified. However, for this initial phase of the methodology, **they are to be considered as relevant material of informational nature only and not as part of the methodological steps.**

A.2.1 Quantifying the direct charges (costs to businesses)

The direct charges quantification
(Regulatory) Charges = Unit cost × Q
where **Unit Cost= the cost of the certification process**
where **Q (for Quantity) = Number of affected stakeholders x Frequency,**
where **Frequency is the number of times that the fee for a certification initiative is required to be paid per year.**

Number of affected stakeholders is equal to the number of businesses answered in the question "Q3: How many (approximately) (potential) producers/manufacturers exist on the market of TOA?" of "STEP 1: DETERMINE THE CONTEXT AND THE SCOPE OF THE TOA", in case the charges are borne by businesses producing/selling the certified product/service/process.

Some (or all) of these charges are zero sums, i.e. a charge for the business and income for the public authority.

A.2.2 Quantifying the administrative costs[6] (costs to businesses)

The administrative costs quantification
Administrative cost for businesses = $\sum P \times Q$
where **P (for Price) = Labour cost + Equipment or supplies' costs; and**
where **Q (for Quantity) = Number of businesses x Frequency,**
Number of businesses is the number of relevant businesses covered under the actual regulation.
The $\sum$ indicates that the costs need to be summed across different types of costs.

The frequency of required actions that generate administrative costs could be one-off or recurring at the determined frequency.

- Relevant cost parameters.
- Labour costs. The parameters to calculate labour costs will be:
    - Time spent on a specific action is usually expressed in FTE of involved organisations to measure the time spent on tasks.
    - Salary could be measured in hourly pay or yearly salary of those performing the action.
    - Equipment or supplies' costs are equipment costs to comply with a certification scheme, in addition to the equipment costs for general production processes. Although we expect that a certification scheme does not require getting new equipment, it might still occur for example that types of equipment and supplies could be necessary to set-up and run procedures to comply with a cybersecurity initiative. The cost parameters will be the acquisition price and the depreciation period.

If the information/actions are actually already part of "business-as-usual" practice, then those should be subtracted from the costs here.

[6] The approach to quantification of the administrative costs for businesses is the so-called Standard Cost Model. The cost model distinguishes between the administrative costs and administrative burdens. For simplicity, only the term 'administrative costs' is used, which actually refers to administrative burdens. For more information and examples, please refer to SWD(2017) 350 Better Regulation Guidelines, Tool #60 THE STANDARD COST MODEL FOR ESTIMATING ADMINISTRATIVE COSTS, available at https://ec.europa.eu/info/sites/info/files/file_import/better-regulation-toolbox-60_en_0.pdf.

If the information is not possible to quantify, it could be assessed qualitatively. For example by completing the following affirmations with one of the suggested qualitative options: ("very little / hardly", "somewhat", "satisfactorily", or – "well") Where "authority", in the sentences below, we refer to the authority in charge of administering and enforcing the certification initiative:

1. The data the authority expects me to provide are _____in line with the data from my own operating process which I already have available.
2. The way in which I am expected to provide the data to the government is _____ in line with how I have them available
3. I understand _____ why the government wants to have this information from me.
4. I understand _____ why the government asks these details from me at these intervals.
5. The government ensures _____ that I have to supply my data only once.
6. The amount of data asked by the government is _____ proportionate to the purpose.
7. This request for information has been worded in a way that every businessperson / employee is _____ able to carry it out.

A.2.3 Quantifying the other compliance costs (costs to businesses)

The other compliance costs quantification
Other compliance Costs = $\sum P \times Q$
where **P (for Price) = Labour cost + Equipment or supplies' costs; and**
where **Q (for Quantity) = Number of affected businesses x Frequency,**
where **Frequency is the number of times that the specific type of costs is required to be paid per year.**
The $\sum$ indicates that the costs need to be summed across different types of costs.

Similarly to the other types of costs, it is a sum of different types of costs, which are calculated as a multiplication of the labour and equipment costs and number of businesses impacted.

A.2.4 Quantifying the Administration and Enforcement costs (costs to the authorities in charge of administering the cybersecurity initiative)

Following the same approach as to the direct costs to businesses, the direct costs for authorities in charge of administering the cybersecurity initiative (usually public authorities) can be estimated first by defining the activities required to implement and enforce legislation, then estimating their frequency and their cost (excluding the business-as-usual costs). Potentially different authorities might be involved, then all the costs need to be calculated and summed.

These costs can vary significantly from option to option and from Member State to Member State. Moreover, it is important to keep in mind that the costs incurred might differ for different authorities: while private control organisations, for example, in case of a voluntary initiative, will charge market fee rates, public authorities might be able to apply some cross-subsidization by using tax incomes to compensate (a part of) the monitoring and compliance costs.

Annual budget data is usually the source that provides data to distinguish between relevant administration and enforcement costs. However, it is also possible that the potential costs are not accounted in the budgets and might require substantial effort in calculating them.

If it is difficult to quantify this type of costs, a qualitative assessment could be performed by answering the following questions:

- Does a (new) certification initiative require the creation of new enforcement mechanisms or institutions, or would it rely on the existing enforcement mechanisms?
- Does the form of the certification initiative have an impact on the size of the costs? If yes, would they vary significantly between different forms?
- Is the expected size of the administration and enforcement costs large that it might mean that one of the forms of a cybersecurity initiative is preferred?
- What kind of costs are driving the size of the administration and enforcement costs? The checklist of potential costs borne by authorities could be used here to identify such cost drivers.

A significant risk of double counting the costs arises in relation to this type of costs. Most likely, these costs will be recovered from regulated businesses or citizens via the direct charges. We suggest to calculate the full costs for public authorities at this step. Where there is a clear intention to recover some or all of these costs through the direct charges, calculations of the expected revenue can also be made and should be included under the business (or citizen) cost categories as appropriate. However, if this is done, it is important to clarify what is the net cost to the public sector, as well as the gross cost. By doing so, you distinguish between:

- The total cost to authorities for administration and enforcement;
- The costs that are expected to be recovered by imposing charges on businesses;
- The full cost to businesses of the compliance with a cybersecurity initiative, including the direct charges.

A.2.5 Quantifying the indirect costs

These costs concern less tangible costs compared to the direct costs and therefore it is usually not quantifiable. They also have a broader impact on the society. This could entail the impact for related markets, for actors that are not directly targeted by the cybersecurity initiative or the society at large.

It is possible (and likely) that the indirect costs are to be the same between different forms of a cybersecurity initiative. If they are different, these costs need to be assessed qualitatively. If different forms or options of cybersecurity initiative are considered, they can be assessed as incremental to each other. In general these questions could be used to assess the indirect costs:

- Does (any of the options of the) cybersecurity initiative create indirect compliance costs?
  - This could mean that additional costs are imposed by a certification initiative (or one of the options of it) that lead for example to restrictions of output, higher downstream prices or any other additional cost for economic agents other than those targeted by the cybersecurity initiative;
- Does (any of the options of the) cybersecurity initiative lead to substitution effects?
  - For example, would citizens or businesses other than the regulated entities shift to alternative sources of supply? Would citizens or businesses other than the targeted businesses shift to alternative modes of consumption?
- Does (any of the options of the) cybersecurity initiative lead to increased transaction costs?
  - For example, would it increase the cost of negotiations between various parties, the costs of information gathering for users, the costs of looking for a different supplier?

- Does (any of the options of the) cybersecurity initiative result in a reduced competition or market access on the market of the TOA or reduced investment or innovation?
  - For example, the following might be considered: the cybersecurity initiative makes it more difficult for new businesses to enter the market of the TOA or it prevents businesses from competing aggressively between each other, or businesses collude on the market of the TOA and therefore it becomes potentially detrimental to end users.

A.3 QUANTIFYING THE BENEFITS

In general, benefits due to a cybersecurity initiative (or any policy initiative) are more difficult to quantify compared to the costs, since they are less tangible. Nonetheless, some of the categories of benefits could be quantified. Most likely different options of a cybersecurity initiative result in very similar benefits with primarily varying costs. If that is the case, the benefits could be assessed qualitatively. One way to quantify the benefits could be to quantify those businesses for whom the harm, that a certification initiative aims to solve (in case of market assessment) or was introduced to solve (in case of impact assessment), would be reduced if a certification initiative were to be introduced or was introduced.

A.3.1 Quantifying the improved market efficiency

Usually this category of benefits is expressed in cost savings. This could be assessed with the same steps as the calculation of direct costs, when a certification initiative leads to a reduction in the direct charges, reduction in compliance costs and/or administration and enforcement costs (steps 1-4 on quantification of direct costs).

Other type of benefits in this category could be the increased willingness to pay for a certified (or complying with the cybersecurity initiative) product/service/process. This goes hand in hand also with stimulating innovation and technological progress, improving information available to users and other market players. Such non-market benefits are often valued using techniques which capture the sum of individual preferences, which are themselves modelled using techniques such as willingness to pay or, alternatively, via simulated experiments observing what people would actually do in different future situations as opposed to what people think they will do.

A.3.2 Quantifying the indirect benefits

Indirect benefits concern individuals and business that are not targeted by a certification initiative and take advantage of positive effects due to business complying with the initiative. These might be difficult to quantify, therefore the questions below provide guidance on what kind of information is being targeted:

- Does (any of the options of the) cybersecurity initiative lead to indirect compliance benefits (“a positive externality”)?
  - For example, a common standard could be introduced in a certain sector that might generate important savings for downstream players; legislation that imposed interoperability between standard interfaces for applications installed on smartphones might reduce development costs for app developers; etc. these benefits have to be assessed and, where possible, monetized.
- Does (any of the options of the) cybersecurity initiative result in macroeconomic benefits spreading to other sectors?
  - If the expected macroeconomic benefits are expected to be significant for the whole economy, it could be estimated using partial or general equilibrium models for quantification of the results. The results then will constitute net benefits (benefits minus costs). Usually these models rely on a lot of assumptions and require a lot of data for each

sector and on how sectors are linked. They also rely on the publicly available data for the whole economy and follow NACE Rev.2 sector classifications that do not allow to create distinction between IoT markets for example. Unless these models are developed internally, an external party needs to be contracted to perform an analysis requiring this modelling.

- Does (any of the options of the) cybersecurity initiative lead to other non monetizable benefits? For example, demonstrating compliance to legal obligations or cybersecurity practises that are considered as best practises.

A.3.3 Single market considerations and Acting at the EU level7

A specific type of benefits can occur when you're considering acting at EU level. This concerns options or initiatives that have an impact of the Single Market, particularly when the initiatives lead to the harmonisation of national frameworks (legislation). Therefore benefits could arise when national framework is fragmented and inconsistent, and action at EU level is taken to harmonise it. Therefore businesses that would like to trade cross-border, would not have costs such as:

- Compliance with national frameworks;
- Adjustments of standards or personnel to deal with national requirements;
- Additional administrative costs to provide other information (for example, additional paperwork).

Once those companies enter cross-border markets, they can benefit from economies of scale, leading to a stronger competition on those markets.

While there could be clear benefits for such type of companies, the harmonisation might result in significant adaptations and changes for certain Member States. For example, when there is an existing certification scheme in France and a completely different certification scheme is introduced at the EU level, it would mean that the national framework in France has to completely change and adjust to the new EU certification scheme.

The quantification of the impacts of such a policy could be rather abstract, therefore seeking external advice is suggested. Specific questions that could guide identification of such an impact could be:

- Is the regulatory framework on cybersecurity harmonized?
- Do businesses and end users face different cybersecurity requirements in each Member State?
- Are certain requirement more cumbersome for foreign companies?
- If a certification initiative is imposed at the EU level, will it lead to increase or decrease in choice for end users? Will there be more competition? Will it lead to improvement of the cybersecurity performance for the whole EU?

[7] Further guidance could be found in SWD(2017) 350 Better Regulation Guidelines, Tool #21 IMPACTS ON THE INTERNAL MARKET, available at https://ec.europa.eu/info/sites/info/files/file_import/better-regulation-toolbox-60_en_0.pdf.

B ANNEX: CHECKLIST OF POTENTIAL ACTIVITIES PER TYPE OF COST OF A CERTIFICATION INITIATIVE

The following checklist includes a wide range of costs that are typically incurred by business, public authorities and citizens respectively:

Type of costs	Example of a cost
Costs borne by Businesses	
Administrative costs	Reporting/giving notice to the authority in charge of enforcement
Administrative costs	Familiarising oneself with the regulatory requirements
Administrative costs	Assessing options (including benefit/cost assessment)
Administrative costs	Choosing an option and developing a compliance strategy
Administrative costs	Applying for a certification
Administrative costs	Time spent on cooperation with authority in charge of granting/enforcing obligations
Administrative costs	Information provision (e.g. for disclosure based regulation)
Charges	Fees, levies, taxes, cost of a certification (some or all of these charges are zero sums, i.e. a charge for the businesses and income for the public authority)
Other compliance costs	Procuring equipment if required
Other compliance costs	Staff recruitment and/or training
Other compliance costs	Purchase of external services
Other compliance costs	Changing production, warehousing and/or distribution processes
Administrative costs	Monitoring/audit of compliance and review of compliance performance
Other compliance costs	Design and implementation of any needed changes to the compliance strategy.
Opportunity costs	Costs incurred due to the need to divert expenditures to compliance and away from preferred uses

Type of costs	Example of a cost
Costs borne by Public authorities or other authorities in charge of administering a certification initiative	
Administration and enforcement	Familiarising oneself with the provisions of the regulation
Administration and enforcement	Designing implementation systems
Administration and enforcement	Developing and implementing staff training
Administration and enforcement	Adapting internal processes
Administration and enforcement	Procuring goods and services and/or recruiting additional staff
Administration and enforcement	Developing and publishing and publicising guidance material for regulated parties
Administration and enforcement	Preparing official notices
Administration and enforcement	Providing advice in response to inquiries, holding preliminary discussions with applicants
Administration and enforcement	Receiving and processing applications
Administration and enforcement	Carrying out formal checks on applicants, examining and compiling data and information − performing checks for completeness
Administration and enforcement	Confirming receipt of data/information or obtaining missing data/information
Administration and enforcement	Carrying out content-related checks, calculations and evaluations
Administration and enforcement	Holding internal or external meetings (e.g. hearings)
Administration and enforcement	Filling in or completing forms, recording data, making classifications − Checking and, if necessary, correcting results/calculations
Administration and enforcement	Receiving payments
Administration and enforcement	Issuing licences/permits
Administration and enforcement	Record-keeping
Administration and enforcement	Transmitting and publishing data
Administration and enforcement	Finalizing information
Administration and enforcement	Implementing monitoring and supervisory measures, classifying risks.
Costs borne by Citizens	
Indirect costs	Familiarising oneself with the obligation
Indirect costs	Obtaining advice (e.g. helpdesks, local administration, lawyer)
Indirect costs	Gathering and compiling and processing data and information (e.g. printed forms, documentary evidence, photos)
Indirect costs	Filling in forms

Type of costs	Example of a cost
Indirect costs	Drafting correspondence (e.g. letters, faxes, e-mails)
Indirect costs	Transmitting information or data to competent authorities
Indirect costs	Making payments
Indirect costs	Photocopying, filing and storing documents
Indirect costs	Co-operating in an inspection by public authorities (e.g. general safety inspection for automobiles)
Indirect costs	Purchasing equipment
Indirect costs	Personally providing certain services or commissioning them to third parties
Indirect costs	Verifying the implementation of obligations
Indirect costs	Time expenditure for travelling and waiting (e.g. at an agency/public authority).
Costs borne by The whole economy (indirect costs)	
Negative market impacts	Reduced competition and inefficient resource allocation
Negative market impacts	Reduced market access
Negative market impacts	Reduced investment and innovation

C ANNEX: LIST OF VARIOUS METHODS TO GATHER INFORMATION ON COSTS AND BENEFITS

Table below presents an overview of different methods that could be used to gather information on potential impacts, costs and benefits that a certification initiative could have on the market.

Method	Application	Advantages	Limitations and risks
Survey	The questionnaire for the survey could contain information on direct labour costs (wage or salary costs), overhead costs, material costs or any other type of costs and benefits that could be foreseen. The averages could be calculated for any type of sector or industry in question.	• Depending on the response rate and representativeness of the results, questionnaires can be used for generalisation or approximation to larger population beyond the sample or a population of stakeholders in a similar sector or industry. • Questionnaires make it possible to gather a large amount of data in a relatively short period of time and with relatively limited costs. • Online questionnaires can incite high rates of participants, as they are often seen as not taking up too much time.	• A survey can be quite time consuming for the surveyed stakeholders or require gathering information that they don't have at hand. • It may be difficult to obtain a good response rate from the relevant stakeholder group. Often respondents lack motivation to respond. Respondents might therefore not reply and the researcher risks a low response rate, potentially impacting the representativeness of the sample. • If the questionnaire is not well designed and sufficiently clear there is a risk for misinterpretation of questions and options by the respondents with the consequential risk of lack of consistency between responses.
Interviews	The questionnaire could contain the same information as in a survey questionnaire; however, most likely only qualitative information could be gathered.	• Interviews can combine structure with flexibility. Especially in comparison to surveys, interviews offer the opportunity to obtain clarifications of incomplete and ambiguous answers. • Information is generated in an interactive manner between the researcher and the interviewee, which makes the interview dynamic in nature. • The researcher uses a range of probes and techniques to actively achieve depth of answer in terms of penetration, exploration and explanation.	• Interviews with open-ended questions produce less statistically valuable data and may not be the right tool for obtaining representative results. They are hence not the ideal tool to collect quantitative data from stakeholders. • Information collected through different interviews, especially less structured ones, might not be comparable and can be hard to aggregate. • Interviews are a time-consuming tool in terms of resources needed to set practical arrangements, particularly if conducted individually. • The interviewer needs a thorough understanding of the topic close to the level of the interviewee, to be able to identify the most relevant and precise questions, and to know when to ask follow-up questions. When working on a new subject, gaining deep knowledge on the topic before engaging in interviews can be challenging.

Method	Application	Advantages	Limitations and risks
Delphi method[8]	The Delphi method could be applied to gather information on costs and benefits when such information does not exist or is very hard to find or the sources of it are questionable. A questionnaire could be drafted for a number of geographically spread experts in certain fields (like sector experts) to gather such information. The collective decision is drawn on the basis of a number of iterations.	• Even though experts might be aware that they participate in a Delphi method together, anonymity of answers ensures that none of experts is influenced by somebody else's opinion. • This method offers a great possibility to gather data when statistical sources, academic and grey literature do not provide needed information or when there is no agreement among experts. • It could be an alternative to studies and reports that require payments. Though it could be weighted.	• It could be time consuming to gather information from the experts and feed it back to the whole group. • Continued commitment is required from the experts who answer the questions through multiple iterations. • The reliability of results or answers of experts could be questioned, as there is most likely no evidence for the views that experts express.
Assessment of a willingness to pay through stated and revealed preferences[9]	This method allows to assess the impact on citizens and consumers through analysis of behaviour or by asking users on their preferences regarding certain changes in the regulatory environment.	• This approach relies on the design of questionnaires, and conducting surveys, therefore the advantages are similar to the ones described above for the survey.	• These methods could be rather theoretical and time consuming. • Organising a setting where consumers indicated what they would do hypothetically might not yield the results that could actually happen in practice, therefore the construction of a questionnaire is very important.
Determining costs and benefits from secondary sources	Methods described above could be difficult to implement because of time or resource constraints. Therefore the impacts estimated as part of another research, report or study could be used as a proxy.	• Low cost approach for obtaining quantitative and qualitative information. • It could be robust when multiple sources are used.	• It should be treated with caution and properly justified. It requires documenting assumptions and perhaps might require further adjustments.
Modelling, for example computable general equilibrium models	Modelling could be used to predict the amount of net benefits (benefits minus costs) generated by a certain regulatory intervention.	• Models are designed to analyse how changes in one industry, market or region lead to a reallocation of resources among several dimensions like sectors and countries. • The models are particularly helpful when expected spill over effects are significant. • It relies on pre-existing data that are available from most national statistical offices.	• This could be very resource and time intensive. It relies on models, which if not developed in-house, require contracting external experts to run the models. • The models rely on a number of assumptions and are very data intensive.

[8] https://research.phoenix.edu/content/research-methodology-group/delphi-method
[9] Revealed preferences method refers to observing what consumers would pay to achieve a certain outcome; while stated preferences assessment refers to asking consumers directly how much they would be willing to pay to achieve a certain outcome in the future. More details and examples are available in Pearce, D. and Ozdemiroglu E., et al. (2002), Economic Valuation with Stated Preference Techniques: Summary Guide, Department of Transport Local Government and the Regions, UK, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/191522/Economic_valuation_with_stated_preference_techniques.pdf

D ANNEX: POTENTIAL DATA SOURCES

One of the obvious challenges of a market analysis in any digital field is the lack of good quality, public data in a lot of cases. For more traditional and stable markets, data sources such as Eurostat, the OECD, or the various national statistics offices can provide a solid basis upon which to understand the overall size of a market in terms of turnover, employment, and other relevant factors. But the purpose of these public data sets is to understand macro-level developments in the economy, and public data sets also tend to defer to collecting information over relatively long timeframes. This can lead to data being collected and collated into categories that do not have much use in a fluid market.

As an example, the European Commission, through the statistical body of Eurostat, classifies a lot of the data that it collects along the *Statistical Classification of Economic Activities in the European Community / Nomenclature Générale des Activités Économiques dans les Communautés Européennes*[10], commonly referred to as NACE, a scheme that has not been revised since 2006. Many ICT activities are categorised under category J, which is "information and communication". Categories here are quite large and fail to capture any nuance in the market. Just a few examples of categories in the scheme include:

J58.2 - Software publishing
J58.2.1 - Publishing of computer games
J58.2.9 - Other software publishing

J61 - Telecommunications
J61.1 - Wired telecommunications activities
J61.1.0 - Wired telecommunications activities
J61.2 - Wireless telecommunications activities
J61.2.0 - Wireless telecommunications activities

J62 - Computer programming, consultancy and related activities
J62.0 - Computer programming, consultancy and related activities
J62.0.1 - Computer programming activities
J62.0.2 - Computer consultancy activities
J62.0.3 - Computer facilities management activities
J62.0.9 - Other information technology and computer service activities

J63 - Information service activities
J63.1 - Data processing, hosting and related activities; web portals
J63.1.1 - Data processing, hosting and related activities
J63.1.2 - Web portals

With this critique offered, there are some public data sets that provide unique and specific data for particular markets. The International Telecommunication Union (ITU), a United Nations (UN)

[10] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Statistical_classification_of_economic_activities_in_the_European_Community_(NACE)/fr

agency specialised in ICT, provides relevant and quoted statistics on telecommunications, broadband and broadcasting.

While some higher level studies managed to use public data sources to conduct their analysis, the more relevant and specific articles that were categorised as a part of the analysis either used their own data sets - not all of which were of clear quality or gathered in a methodologically transparent way - or were based on survey data. The latter category seemed to be the most consistent way that market analyses in this field collected data, drawing often on proprietary surveys.

Another familiar means to collect data was via national associations and cybersecurity authorities, which is a common way to get access to data. One challenge of this source of data, particularly from associations, is that the data they share will tend to support a particular viewpoint and access to this data can often depend on whether the association feels that a report will fall within their interests. It may also be selective and can also lack transparency, which introduces questions of bias (how many companies were surveyed, what size, what geographical spread and many other questions).

Finally, there are private data sets that are collected by well-established firms, which are sold to governments and consultancies for analysis. Private-sector datasets tend to provide the greatest level of specificity, given that other private companies use them to make business decisions, but they also create challenges for market analyses that are used in a public sector setting, namely:

- The costs for accessing private-sector datasets can be quite high.
- Private-sector datasets can come with Intellectual Property Right (IPR) restrictions, meaning that certain details cannot be published, which may not be feasible in a public-sector context where the results of a market analysis need to be shared with stakeholders and even the general public.
- Working with private-sector datasets works better in cases where the market analysis is a one-time exercise. In some cases, it can be useful to conduct the same analysis several times to understand how the market is evolving, and this comparison works best if the methodology can be replicated across studies. This means that the same datasets should be used, which means continually purchasing datasets from the same vendors. This creates vendor lock-in, and the potential for vendors to exploit their position for financial advantage.

TP-01-21-111-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. For more information, visit www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-500-5
DOI: 10.2824/919706