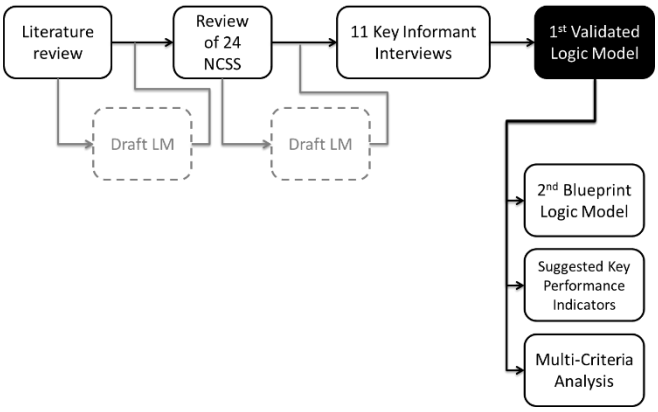
Annex B – Methodology

This project used a combination of three empirical techniques (that is: 1) literature and document review of NCSS 2) 11 Key Informant Interviews and 3)logic modelling developed through internal interactions in the study team.

A brief survey of the literature conducted by manual search using terms including 'evaluation' + 'cyber-security' allowed exploration of the role that evaluation plays in complex public policy interventions like the design and formulation of a NCSS. Publicly available declaratory policy regarding NCSS were then reviewed, analysed and classified in order to identify evaluation components and derive a mapping of such components.

Finally, evidence was gathered from 11 Key Informant Interviews (KII)s with a self-selected sample of practitioners. The purpose of these interviews was to investigate the presence of key performance indicators in respective NCSS and to validate draft versions of a logic model produced as one of the key outputs of the work. Evidence from these empirical activities was used at various stages to inform the development of two logic models.

The first logic model captured existing examples of the inputs; activities; outputs; short and long term outcomes and impacts into a single meta-picture of publicly available NCSS. These elements of individual logic models of NCSS were subsequently aligned with the headings of the EU Cyber Security Strategy (Achieving cyber resilience; developing cyber defence; reducing cybercrime; developing the industrial and technological resources for cyber-security; secure critical information infrastructure.



The second, generic 'blueprint' logic model was developed to directly assist policy practitioners charged with designing, implementing or evaluating their NCSS. The blueprint comprised separate but related elements:

1. A model reflecting a possible range of content-related inputs; activities; outputs; outcomes and impacts and;
2. A model reflecting specific operational or programme management orientated inputs; activities; outcomes and impacts governing the design, implementation and evaluation of a NCSS.

Each iteration of the logic model was derived through internal study team discussion, taking the evidence from each phase into account. Each logic model was created according to the top level headings of the 2013 EU Cyber Security Strategy.

Finally, a set of suggested key performance indicators reflecting the heading; measurable indicator and possible sources were identified and allocated to each element in order to offer assistance to practitioners in developing and evaluating the NCSS.

Logic Model

The development of a evaluation framework of a NCSS needs to make explicit the assumptions about how and why an intervention will work and with what outcomes for the framework In this evaluation approach, we will use a tool called logic modelling.[1] By looking at these aims and at the associated building blocks in the programme implementation process, those engaging in an evaluation can seek to identify what the key 'ingredients' of a given initiative are. The model also helps policymakers reflect on the assumptons upon which their plans are dependent; the risks related to the realisation of the program's objectives and the conditions which are necessary for the planned results to materialise.

The blueprint logic model illustrates the building blocks that can be used to map the "logic" behind the actions taken and how these support the goals of the NCSS. This tool can be used to detect and summarise the relationship between the inputs, processes, outputs and outcomes involved in the strategy. The streams of activity in the blueprint logic model have been defined in a manner that allows Member States to align the articulation of their strategy to the overall goals of the European Cybersecurity Strategy. However, national contexts vary greatly across Member States. Therefore, the structure contains only suggestions for potential elements and clusters to take into account without prescribing in detail what these areas of activity should contain and what kind of relationship should persist between the individual elements.

Due to the schematic nature of this approach, some of the connections between constructing blocks may become necessarily simplified. Certain elements, for instance loops where outcomes or outputs of a process form inputs for another activity, may be challenging to represent. Finally, as this approach depends to a great extent on the success of activities in contributing to objectives of the strategy it is necessary to periodically re-assess logic models as the NCSS is implemented to ensure its relevance and accuracy for evaluation.

1. *Define the place of the logic model in the policy process and put together a team working on the evaluation*
2. *Problem definition*
3. *Capacity/Inputs/Gaps Inventory*
4. *Activities and processes*
5. *Outputs*
6. *Arrange logic model components and review for consistency*
7. *Revise and adapt logic model as the implementation of the NCSS is underway*

Figure 1 Summary of logic modelling process

[1] See e.g., Savaya, R., & Waysman, M. (2005). The logic model: A tool for incorporating theory in development and evaluation of programs. Administration in Social Work, 29(2), 85-103.

Key Performance Indicators

Key performance indicators (KPIs) allow policymakers to track progress towards objectives of the strategy. Two of the 11 interviewed national authorities reported defining indicators of success when planning their strategy. According to the interviewees, these were used in reviewing the activities at the end of a NCSS cycle and in preparing successive iterations of the strategy.

KPIs are a measures selected as a marker of success. They can be defined for activities and desired outcomes, outputs and impacts that will have an impact on an organisation's ability to deliver on policy objectives and targets in the future.[2] Incorporating KPIs in the evaluation framework enables the organisation to track progress on the initiative as well as motivate contributions. However, care needs to be taken when associating KPIs and setting target values, selection of inappropriate KPI (for instance focusing on localised objectives that do not contribute to the success of the overall strategy) can result in counterproductive behaviour and sub optimised outcomes.[3]

In the context of the toolbox suggested here, the main added value of the KPIs is to monitor progress towards the program's objectives. Relying on the information conveyed by the indicators, policymakers can assess the feasibility of reaching the objectives set at the design phase of the strategy. Indicators can be mapped onto the streams of activity described in the logic model and cover all areas of activity included in it, at all levels (from inputs to outcomes). The list is a suggestion rather than a prescribed set of indicators, aiming to offer a starting point for policy professionals working on the evaluation of their strategy and on engaging stakeholders in the discussion about defining success and measuring outcomes of cybersecurity policy at the national level.

Policymakers and other stakeholders alike have an interest in measuring the impact of the NCSS. This measurement can focus on both policy effectiveness - i.e. to what extent security and resilience has been improved by the implementation of the NCSS and how this has affected the citizens (captured by the outcomes and impact section of the logicmodel); and the efficacy of the process, i.e the extent to which the observed changes can be attributed to the specific elements of the strategy.

In order to constitute valuable indicators, these KPIs will have to correspond to a few fundamental characteristics, stressed in the literature in both policy evaluation and management science.[4]

These indicators share certain features which are summarised in the box below.

Good practice in defining indicators is often described with the SMART acronym:

1. **Specific** – clear and focused to avoid misinterpretation or ambiguity;
2. **Measurable** – can be quantified/measured (although they may be either qualitative or quantitative)
3. **Attainable** – targets are set that are observable, achievable, reasonable and credible under expected conditions and timing as well as independently validated;
4. **Relevant** to and consistent with the specific agency's vision, strategy and objectives;
5. **Time-related –** there is a time-limit on achieving the results.

Some additional characteristics have been proposed for the definition of KPIs[5]:

[2] SAS White Paper of Key Performance Indicators, 2013
[3] Public Record Office Victoria (2010) *PROS 10/10 G3 Key Performance Indicators Guidelines 2010-2015*, Public record office Victoria. http://prov.vic.gov.au/wp-content/uploads/2011/05/1010g3.pdf
[4] See e.g., fn 61-63; 2012 ENISA Best Practice guide
[5] SAS White Paper of Key Performance Indicators, 2013

6.	**Governable**: they are agreed by the relevant people and the roles regarding accountability and responsibility are clearly defined and understood; and
7.	The measured aspect should make a significant **impact** on current or future performance.

Two of 11 interviews conducted for this study corroborated the view that defining indicators that meet these criteria can be a challenging task in the context of cybersecurity policymaking. To certain objectives defined in the strategies, indicators can be linked only approximately, as these outcomes are often also influenced by a multitude of factors external to cybersecurity policy. Furthermore, many of these outcomes are also difficult to measure on the basis of data available to policymakers. Areas where evidence is difficult to obtain include the level of overall security of a country's information systems, as most currently available data sources on data breaches and information security breaches are incomplete or biased.[6]

One relatively straightforward way of developing the key performance indicators builds on the elements identified in the logic modelling. Figure G.1 summarises the steps involved in the process.

Figure 2 Summary of KPI definition process

1. *Map processes and how the actions under the NCSS contribute to realising the goals laid out therein*
2. *Associate one or more indicators to each step of the process*
3. *Associate a success level to each of the indicators*
4. *Review indicators for relevance and consistency with the goals*
5. *Identify mechanism for tracking them and process for reviewing and updating them as the NCSS implementation goes underway*

Validation and verification

The validation of the model is the next phase of this exercise. As you have already seen in section 3 of the document, the logic model was modified (from version 1 to version 2) based on the input and feedback received during the interviews with experts: topics like training and education, critical information infrastructure protection and enhanced CERT capabilities where added in the logic model after the validation process. The logic model has been updated and next was the verification of the new updated logic model. The verification was conducted via second round of calls and email exchange with the experts intervieweed, and the final version was also shared with the ENISA NCSS working group. The final version is presented in the report.

[6] See Robinson and Horvath. (2013)