Annex 1
Summary of selected frameworks for and assessment models of national cyber security strategies

	ITU	CTO	ENISA	CMM	CRI	ASPI	eGA	WEF
Objectives	Providing the right motivation to countries intensify their efforts in cyber security; help foster a global culture of cyber security and its integration at the core of information and communication technologies.	Serve as a guide for countries to develop their individual national cyber security strategies. The guide provides practical advice and proposes actions that can be adapted by countries to suit their individual circumstances.; Indicate where a country lacks intrinsic capacity in aspects of cyber security and potentially needed to reduce risks to national goals or to create opportunities for the country.	Perform a stocktaking exercise on the approaches currently used to perform evaluation of national cyber security strategies; Present recommendations and identify good practices on the implementation and evaluation of cyber strategies; Design and develop an evaluation framework to adapt to the varying needs of countries at different levels of maturity in their strategic planning.	Increase the scale and effectiveness of cyber security capacity building, both within the UK and internationally"; making this knowledge available to governments, communities and organisations to strengthen their cyber capacity.	Inform national leaders on the steps they should consider to protect their increasingly connected countries and potential GDP growth by objectively evaluating each country's maturity and commitment to cyber security and resilience.	Make considered, evidence-based cyber policy assessments; identify opportunities for the sharing of best practice, capacity building and development, plus commercial opportunities. With this additional layer of analysis, governments and the private sector can tailor engagement strategies to best fit existing levels of maturity in each policy area in each country.	To measure the preparedness of countries to prevent cyber threats and manage cyber incidents. A comprehensive cyber security measurement tool that provides accurate and up-to-date public information about national cyber security. Different applications for national cyber security analysis and development will be developed.	To highlight the opportunities offered by ICTs and provide an indication of the ways they are transforming economies and societies around the world.
Typology[1]	Legal; Organizational; Capacity-building; Technical	Strategy [document] components of: Introduction; Guiding principles; Strategic goals and vision; Objectives and priorities; Stakeholders; Governance and management structure; Implementation (covering Legal and regulatory framework; Awareness; Local technical capability; Incident response); Monitoring and evaluation	Cyber defence policies and capabilities; Cyber resilience; Counter-cybercrime; Cyber security support to industry; Critical information infrastructures protection.	Cyber policy and strategy; Cyber culture; Workforce and leadership; Legal and regulatory framework; Risk management thorough organization, standards and technology.	National strategy; Incident response; E-crime and law enforcement; Information sharing; Investment in research and development; Diplomacy and trade; Defense and crisis response	Governance; Financial cybercrime enforcement; Military application; Digital economy and business; Social engagement	Legislation in force – legal acts, regulations, orders, etc. Established units – existing organizations, departments, etc. Cooperation formats – committees, working groups, etc. Outcomes – policies, exercises, technologies, websites, programs, etc.	The networked readiness framework translates into the NRI, a composite index made up of four main categories (*subindexes*), 10 subcategories (*pillars*), and 53 individual indicators distributed across the different pillars.

[1] *Inter alia* notions such as dimensions, components, elements, key performance indicators, or topics. Eric Luiijf and Jason Healey identify "the five mandates of national cyber security" as military cyber operations, counter cyber, intelligence/counter-intelligence, cyber security crisis management and critical infrastructure protection and CIP, and internet governance and cyber diplomacy. The authors notice the "optimal, clean sheet positioning of the cyber security functions" as "a theoretical best practice." (Luiijf & Healey, "Organizational structures and considerations" in Klimburg (ed.), *National Cyber Strategy Framework Manual*, p. 120-128.)

Methods		Forwarding monitoring and evaluation method: Key Performance Indicators by which progress will be measured based on reporting required from stakeholders, collating the data to achieve transparency in reporting progress against the strategy's objectives either as measurements of about delivery activity or measure the outcome or end state by posing questions to those stakeholders who are intended to benefit.	Literary review; Documentation review of national cyber security strategies; Logic modeling where Key Performance Indicators illustrating the underlying logic of recurring components of cyber security strategies are mapped to the objectives of the evaluation model.	Structured 3-5 day workshops and self-assessment focusing on the five dimension and their sub-dimensions, factors and categories. A report with recommendations for courses of action.	Evaluating each country's maturity and commitment to cyber security and resilience with a focus on economic growth; Defining what it means for a country to be "cyber ready" and document the core components of cyber readiness into an actionable blueprint for countries to follow. The fact-based assessments for each country rely on primary sources, and each unique data point is grounded on empirical research and documentation.	Weighed indicators, the importance ratings, and averaged weighting factors that are used in the calculation of an overall score. Each country is rated against the 10 factors. The overall score is the sum of the scores against each factor weighted by the average importance. The overall scores are converted to a percentage of the highest possible score [100].	Identification of national level cyber threats Identification of cyber security measures and capacities Selection of important and measurable aspects Development of cyber security indicators Grouping of cyber security indicators Each indicator has a value showing the relative importance of the indicator in the index. The values are given by the expert group accordingly: 1 point – a legal act that regulates a specific area 2–3 points – a specialised unit 2 points – an official cooperation format 1–3 points – an outcome / product	Successive aggregations of scores, from the indicator level (i.e., the most disaggregated level) to the overall NRI score (i.e., the highest level). Scores for indicators derived from the WEF Executive Opinion Survey are measured on a 1-to-7 scale; all other indicators come from external sources To align them with the Survey's results, a min-max transformation is used, transforming them into a 1-to-7 scale. An arithmetic mean is used to aggregate individual indicators within each pillar and also for higher aggregation levels (i.e., pillars and subindexes).
Measurements	Index (0.000 – 1.000); Global and regional ranking	n/a	n/a	Start-up; Formative; Established; Strategic; Dynamic.	Insufficient evidence; partially operational; fully operational.	Weighed score (0.0-100) Engagement opportunities indicators	The percentage (0-100%) the country received from the maximum value of the indicators regardless of whether indicators are added or removed.	

Sources:

- The International Telecommunication Union, *Global Cybersecurity Index and Cyberwellness Profile,* https://www.itu.int/pub/D-STR-SECU-2015;
- The Commonwealth Telecommunication Organization, *Commonwealth Approach for Developing National Cybersecurity Strategies* (2015), http://www.cto.int/media/foth/cybsec/Commonwealth%20Approach%20for%20National%20Cybersecurity%20Strategies.pdf;
- European Union Agency for Network and Information Security, *An evaluation framework for cyber security strategies*, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1;
- University of Oxford, *Cyber Security Capability Maturity Model,* v. 1.2 (15 December 2014), https://sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf;
- Melissa Hathaway, *Cyber Readiness Index 2.0.* Potomac Institute for Policy Studies (November 2015), http://www.potomacinstitute.org/academic-centers/cyber-readiness-index;
- Australian Strategic Policy Institute International Cyber Policy Centre (ASPI), *Cyber Maturity in Asia-Pacific Region 2017,* https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017;
- e-Governance Academy (eGA), *National Cyber Security Index* (NCSI), https://ncsi.ega.ee/;
- World Economic Forum (WEF), *Networked Readiness Index,* https://widgets.weforum.org/gitr2016/