National Risk Assessments

ENISA Study and Background Analysis

Agenda

- Context and motivation
- Objectives and approach
- Main findings
- Challenges
- Recommendations
- Next steps

National Contingency Plans & Exercises in the Cybersecurity Strategy

- In the European Cybersecurity Strategy the European Commission calls for the development of:

'...*national contingency plans and organise regular exercises for large scale networks security incident response and disaster recovery, as a step towards closer pan-European coordination..'*

National Contingency Plans (NCPs) & National Risk Assessment (NRA)

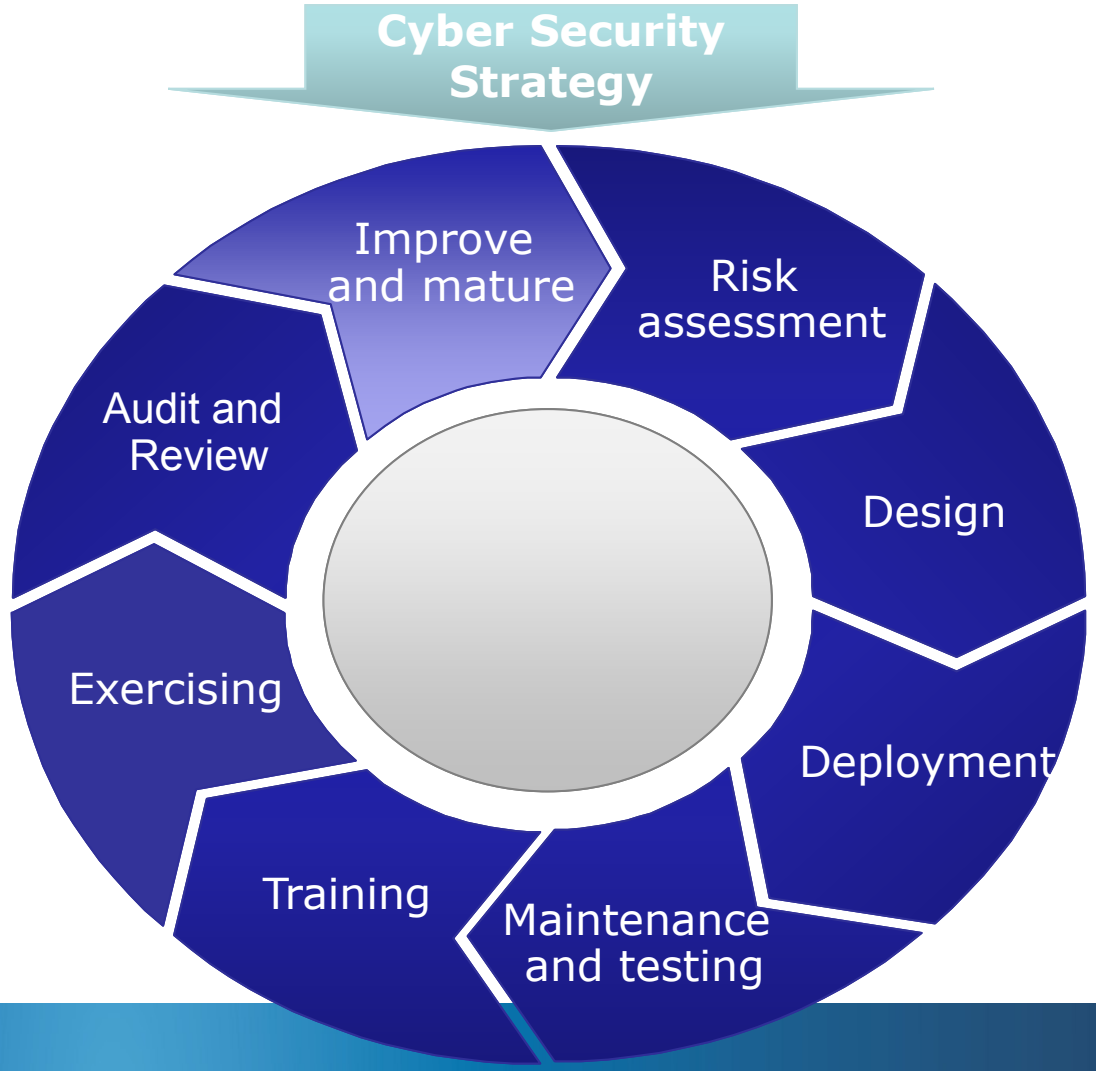
- From the proposed NIS Directive:

"..The national NIS strategy shall include a national NIS cooperation plan complying at least with the following requirements:

(a) A risk assessment plan to identify risks and assess the impacts of potential incidents;

…"

NRAs are inherent parts NIS Co-operation Plan lifecycle (ENISA, 2011)



ENISA work on national plans relevant to cyber security

- 2011 study into National Contingency Plans and Good Practice Guide
- 2012 Good Practice Guide into National Cyber Security Strategies
- Series of International Conferences on Crisis Co-operation and Exercises
- 2013 Analysis and Guide on National Risk Assessments

Objectives

- Capture the main aspects concerning the implementation of an NRA
  - administrative, economic, legal and cultural factors
- Look at the pre-existing state of the art in risk analysis
  - Applicability to national-level scale
- Provide an evidence-based methodology for establishing a NRA programme
- Ultimate goal
  - A step-by-step practical guide for NRA

Approach

- Gather empirical evidence
- Perform interviews and questionnaires
  - 21 organisations from all over the world
- Continued (semi-)structured discussions with experts
- Analyse the challenges and propose recommendations
  - Publish an analysis report (Oct 2013)
- Ultimate goal
  - Pilots and a mature step-by-step practical guide for NRA (2014-15)

Related works

- Somewhat limited documentation exists regarding NRAs..
  - Less so at national level and for cyber

- Risk assessment tools are relatively plentiful in the IT security world (ISO suite; CRAMM; eBIOS)
- The International Risk Governance Council released guidance on how to establish a generic NRA programme
- The EU's Joint Research Centre (JRC) reviewed 19 different NRAs in the context of CIP
- The US National Academies of Science (NAS) reviewed Department of Homeland Security (DHS) NRA approaches

Main findings (1/2)

- Identification of threats and modelling
  - Articulated in a high-level strategy
  - Either qualitatively or quantitatively
  - Based on scenarios
- Approaches to the conduct of an NRA
  - through a formalized framework or approach or
  - based on a decentralised model where each actor prepares their own risks assessment to be integrated by a co-ordinating authority

Main findings (2/2)

- National level methodologies:
  - Scenario based approaches where actors are gathered together to consider threat scenarios and impacts;
  - Qualitative approaches which may describe risks as a narrative or apply simple categories (low; medium; high);
  - Quantitative approaches which apply ordinal thresholds (e.g. a risk is classed severe if it affects 1 in 20,000);
  - Approaches which combine elements of all of the above (for example, using scenarios and then qualitative and quantitative methods.

Key challenges and lessons

- The lack of a harmonised national framework for cybersecurity particularly terminology
- Incomplete and diverse risk assessment methodologies;
- Lack of comprehensive methods to address threats
- Need for effective risk management and preparedness capacity and skills
- Information sharing between different actors involved in an NRA
- Effective collaboration between public and private sectors
- International co-operation (how learned from others)

Recommendations focused towards Member States

- Achieve better understanding of threats and consequences for society
- Better integrate NRAs into NIS Co-operation Plans
- Expand public-private sector dialogue and information sharing to perform NRAs
- Develop and improve national well documented and tested CIIP frameworks, structures and procedures
- Seek guidance and practices from other countries or European organisations

Further recommendations

1. Develop, test and continuously mature a step by step guide on how to perform NRAs
   a) Pilots with interesting countries
2. Establish and share a catalogue of scenarios to could help Member States in their NRAs
3. Establish and strengthen a community of interest of cyber NRA practitioners
4. Facilitate access to EU scientific expertise on NRA
5. Facilitate exchange knowledge of risk analysis expertise with other domains that assess complex cross border risks, such as border security financial services or public health

Next steps

- Step-by-step guide for NRAs (draft)
- We came up with a two phases approach:
  - Preconditions – achieving background understanding
  - Creating, implementing and running an NRA programme
- To be discussed later during the session
- Work more on the guide
  - Create templates for practical use
  - Pilot with interested countries

Questions?

Contact: Panagiotis TRIMINTZIOS, ENISA
panagiotis.trimintzios@enisa.europa.eu

Steps to establishing and maintaining an NRA programme

Introduction and overview

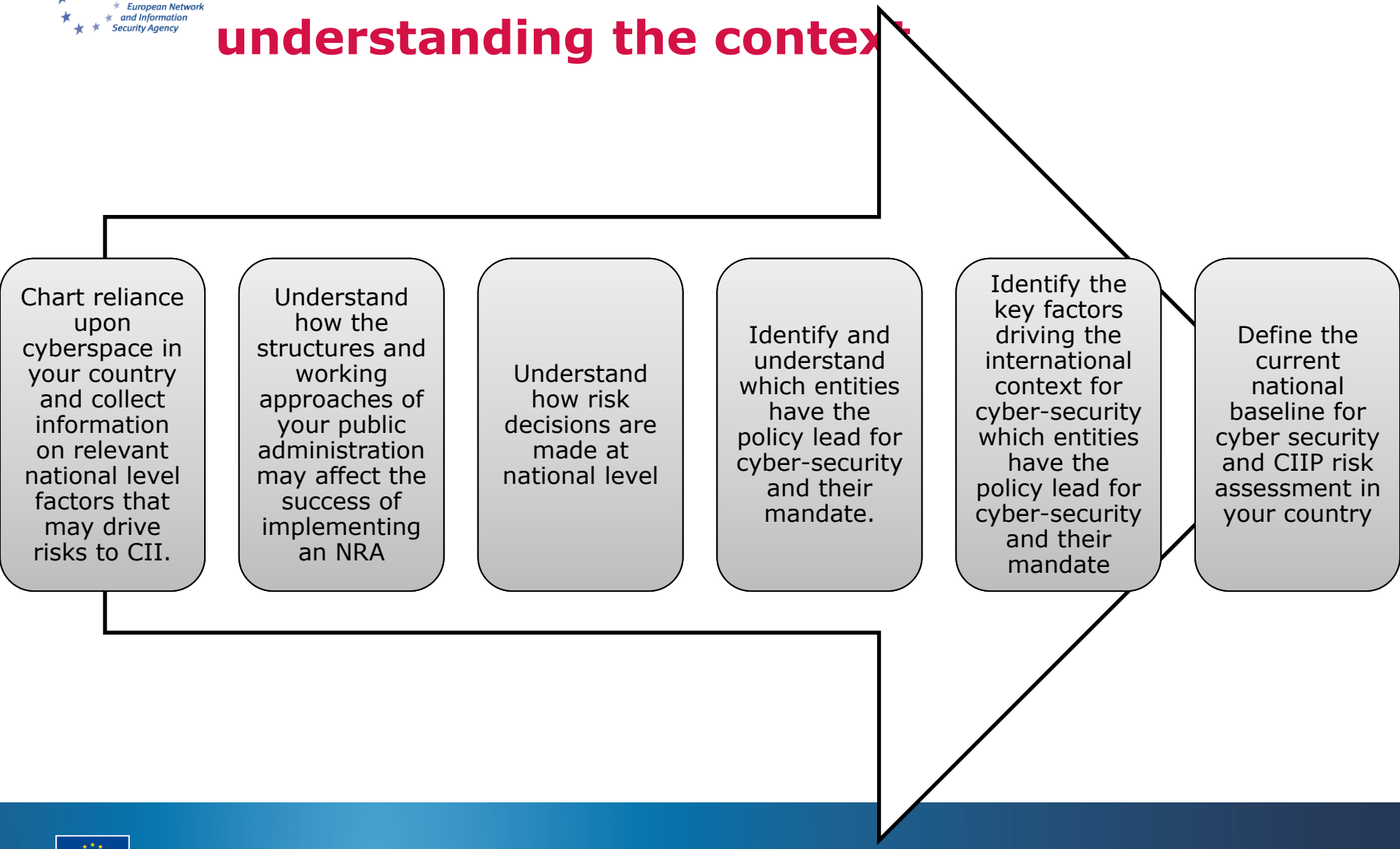
NRA Panel

24th September 2013

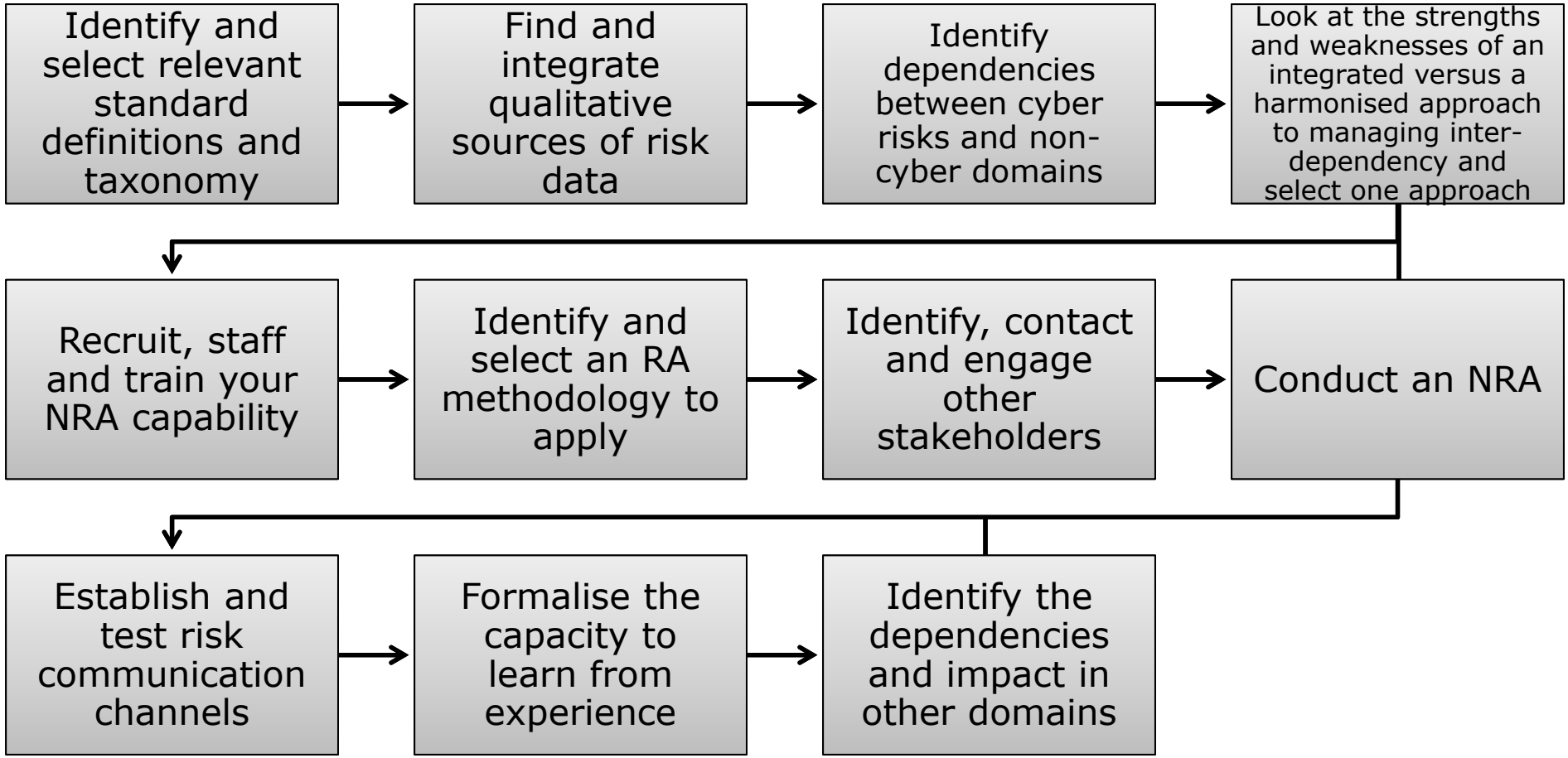
Two phases

- Phase I: Preconditions – achieving background understanding
- Phase II: Creating, implementing and running an NRA programme

Phase I: Pre-conditions for an NRA: understanding the context



Phase II: Creating and implementing an NRA capability



Does this seem sensible & feasible?

- Do the steps seem logical?
- Have we captured all dependencies / prerequisites?
- Are some steps iterative? If so, which?
- Can some steps be undertaken in parallel? If so, which?
- Are the steps mutually exclusive & collectively exhaustive?