ENISA 2008

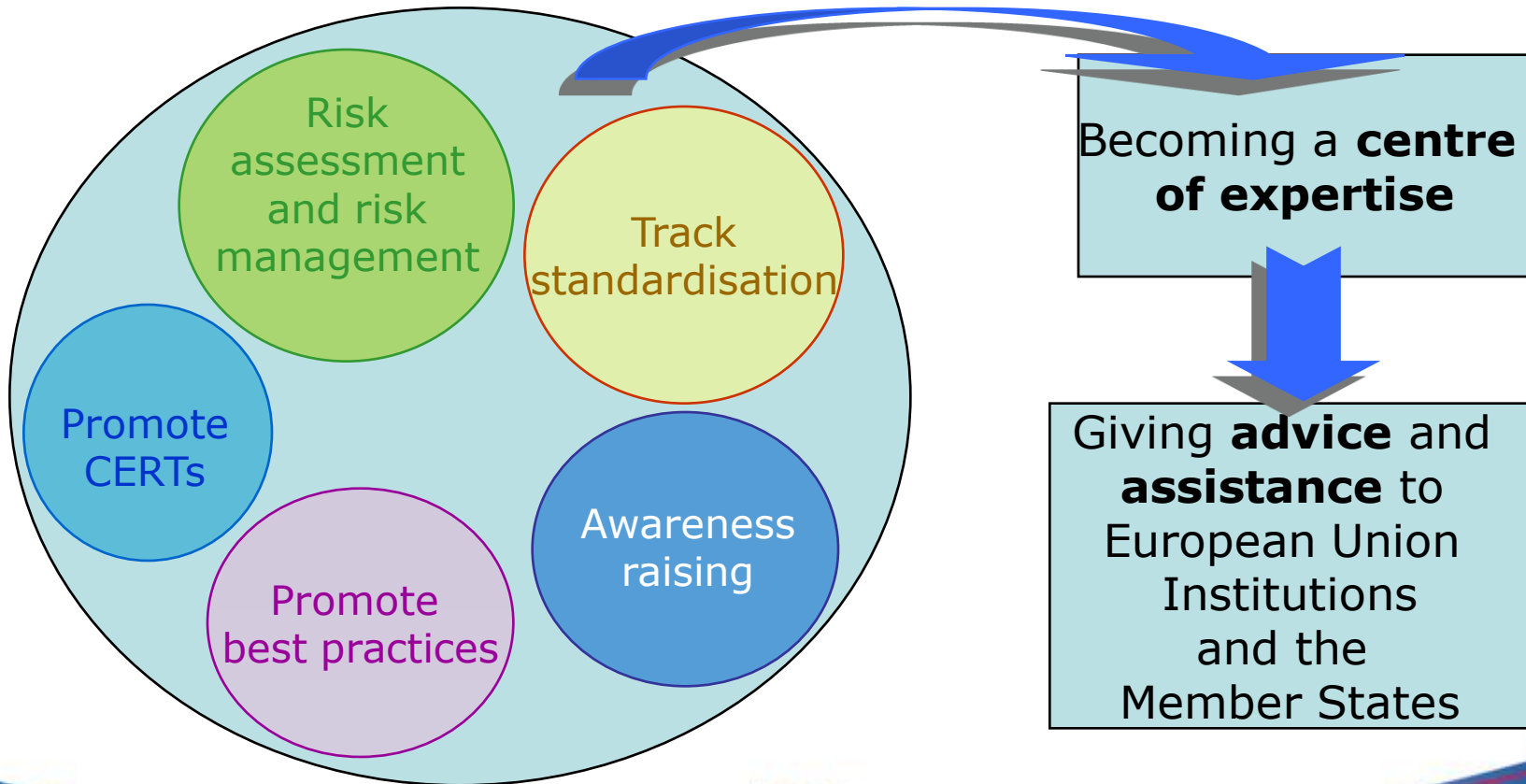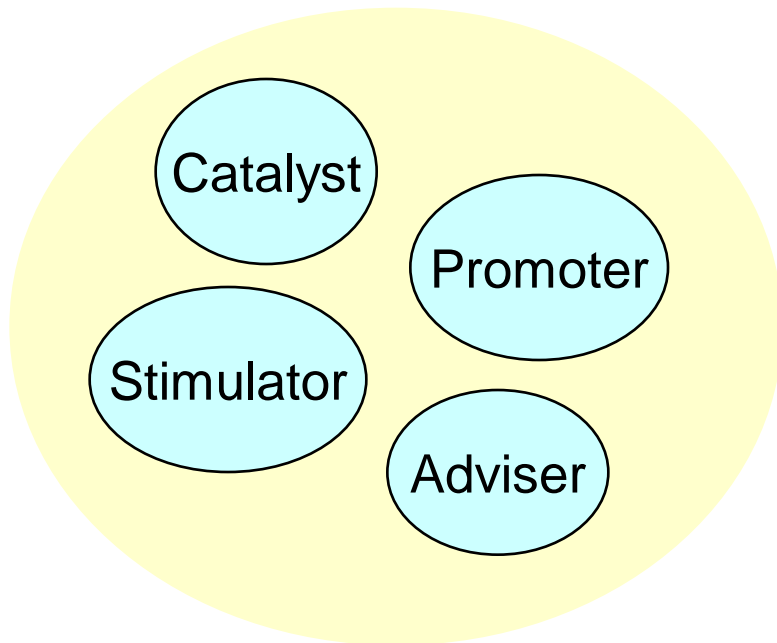## Build on synergies, achieve impact

Outline

★ ENISA structure and context

★ Scope of ENISA

★ Current projects and activities

★ Multi-annual thematic programs

★ Opportunities for cooperation with ENISA

ENISA's main tasks

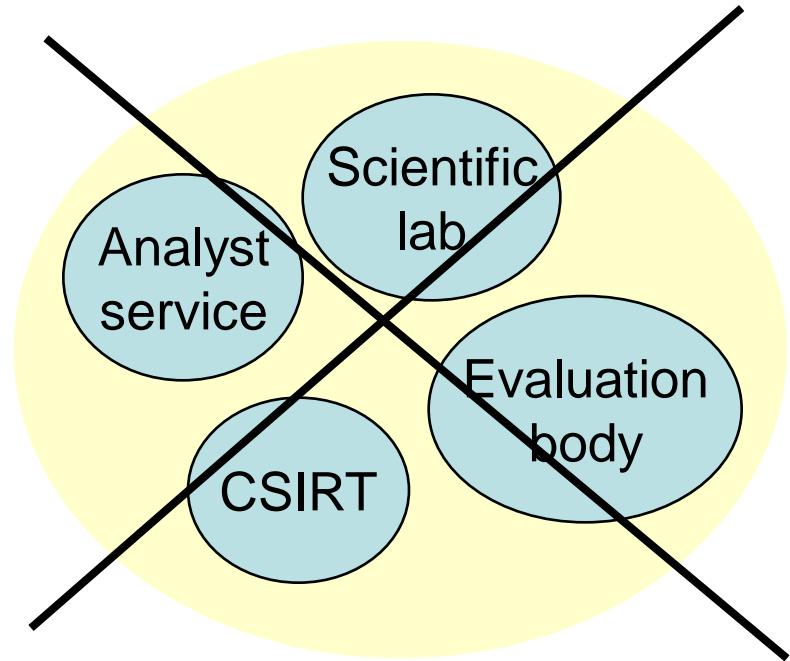Risk assessment and risk management

Track standardisation

Promote CERTs

Promote best practices

Awareness raising

Becoming a **centre of expertise**

Giving **advice** and **assistance** to European Union Institutions and the Member States

Scope of activities

to be a…   and not a…

Catalyst

Promoter

Stimulator

Adviser

Analyst service

Scientific lab

Evaluation body

CSIRT
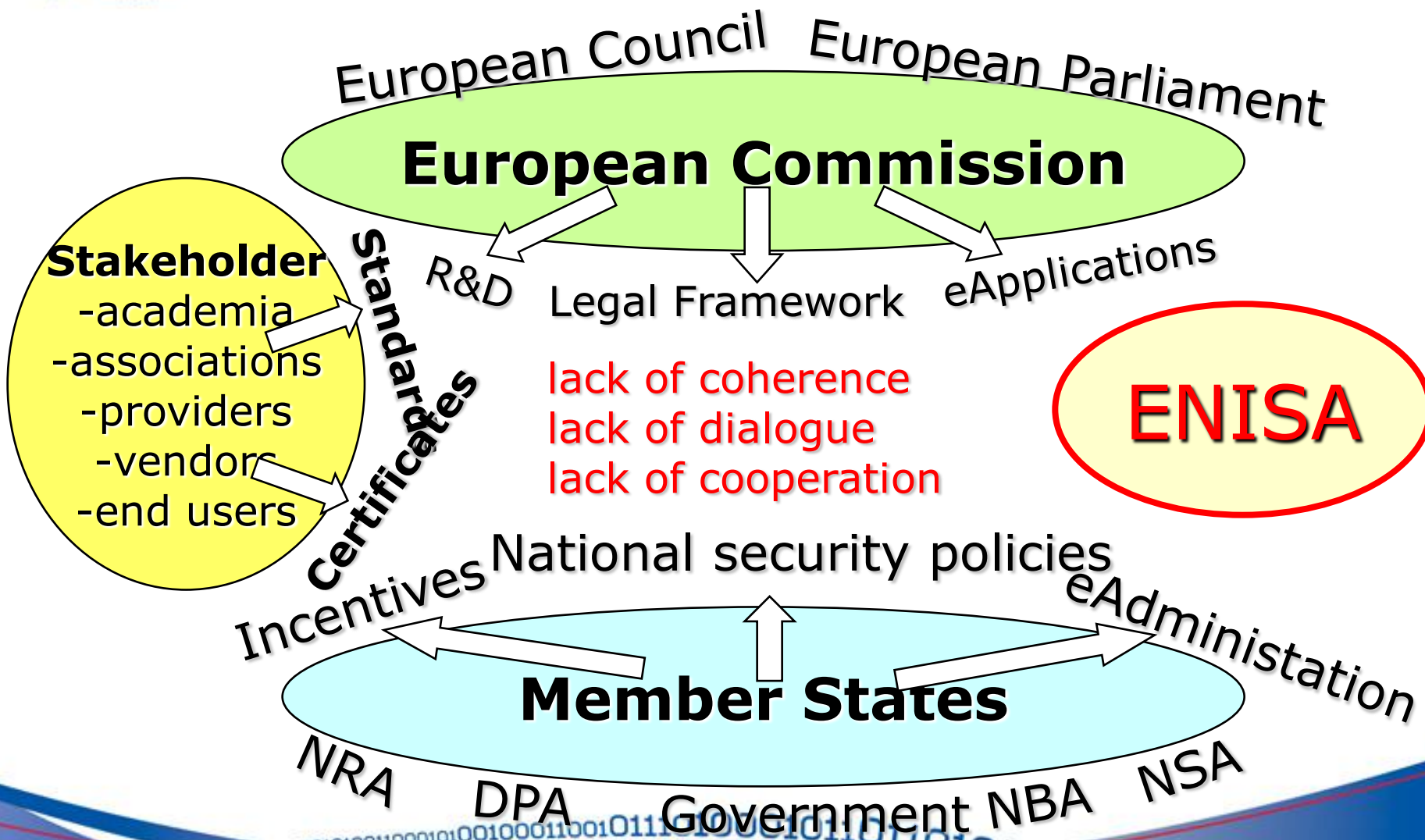
… maintain internal expertise, at **the disposal for EU and Member State competent bodies**
(respond to Requests and Calls for Assistance)

ENISA's Role

European Council   European Parliament

European Commission

Stakeholder
-academia
-associations
-providers
-vendors
-end users

Standards

Certificates

R&D   Legal Framework   eApplications

lack of coherence
lack of dialogue
lack of cooperation

ENISA

Incentives   National security policies   eAdministration

Member States

NRA   DPA   Government   NBA   NSA

www.enisa.europa.eu

Activities for 2008 and beyond

* **Multi-annual Thematic Programmes**
  * Strategic priorities for ENISA
  * Implemented through a number of Work Packages
* **Current focus on:**
  * Improving Resilience in European e-Communication Networks
  * Developing and Maintaining co-operation between Member States
  * Identifying Emerging Risks for creating trust and confidence
  * Building information confidence with Micro Enterprises (Preparatory action)

MTP1 - Resilience

The ability of a system to provide & maintain an **acceptable level of service** in face of faults *(unintentional, intentional, or naturally caused)* affecting normal operation
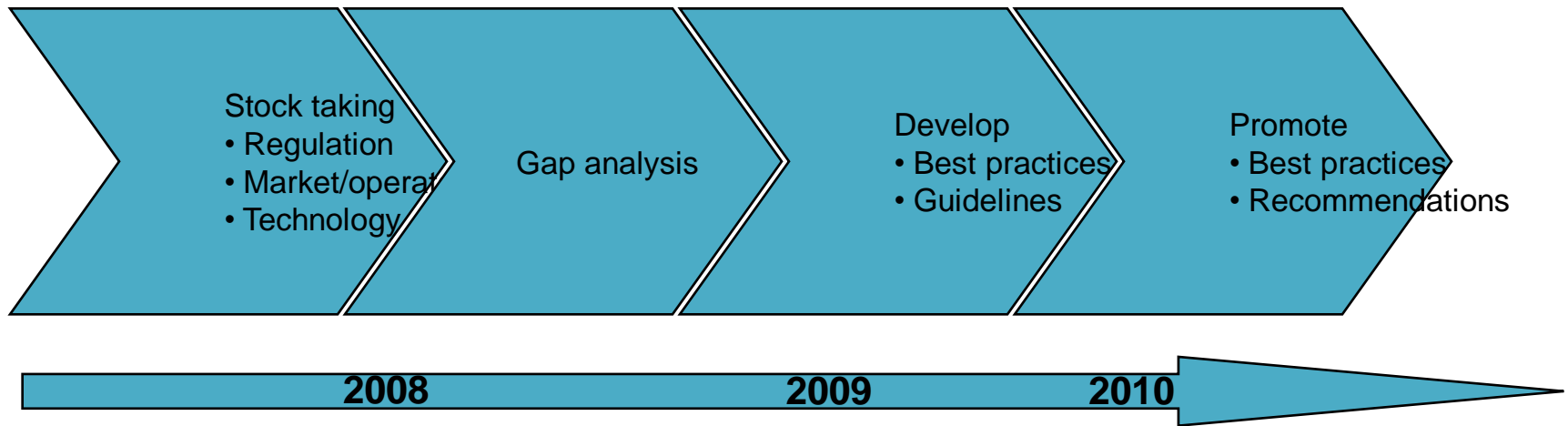
Network resources - resilience

* A resilient network design aims to remove single points of failure in switching/routing equipment;

* The main aim of resilience is for fault to be invisible to users;

* Network availability is an issue of risk management and involves technical measures such as:

    * Resilient design;
    * Resilient transmission media;
    * Resilient equipment;

MTP1 - Improving Resilience in European e-Communication networks

Collectively evaluate and improve resilience in European e-Communication networks

Stock taking
• Regulation
• Market/operat
• Technology

Gap analysis

Develop
• Best practices
• Guidelines

Promote
• Best practices
• Recommendations

2008   **2009**   **2010**

By 2010, the Commission and at least 50% of the Member States have made use of ENISA recommendations in their policy making process

www.enisa.europa.eu

MTP 1 Overview

* WPK 1.1 – Regulators / NRAs
  * Regulations, Rules, Requirements, Responsibility, Liability, Controls
* WPK 1.2 – Network and Service Providers
  * Measures, Best practices, Standards
* WPK 1.3 – SW/HW Providers
  * Standards, Current/emerging technologies

MTP1 – Perspectives '09

★ WPK 1.1 : Gap analysis on regulatory measures
  - ★ Analysis of common approaches and gaps
  - ★ Large consultation of stakeholders and authorities

★ WPK 1.2 : Gap analysis of implemented measures
  - ★ Clustering of implemented measures and resilience approaches
  - ★ Gaps analysis and best practice identification

★ WPK 1.3 : Analysis and recommendations on how to enhance resilience
  - ★ Recommendation on resilience enhancing methods and tools
  - ★ Business impact analysis and incentive proposals
  - ★ Networking trends and impact

MTP 2 – Cooperation

* WPK 2.1 – Awareness Raising community
  * Awareness Raising online portal
  * Building AR community
* WPK 2.2 – CERT communities
  * CERT inventory update
  * CSIRT exercise book

MTP 2 – Cooperation

★ WPK 2.3 – interoperable eIDs

   ★ Gap analysis: IDABC authentication level description using SAML

   ★ Report on eIDM framework

   ★ Position paper on mobile eID

   ★ Position paper on privacy features in eID specs

★ WPK 2.4 – Good Practice Brokerage

Awareness Raising – success stories

★ User's Guide on How to Raise NIS Awareness

★ Information Security Awareness Initiatives: Current Practice and the Measurement of Success

  ★ What governments and private companies are currently doing to assess the impact and success of awareness raising activities?

  ★ Focus on sets of metrics and key performance indicators, can contribute to the development of a wider culture of security

  ★ Ongoing translation to ALL official EU languages

CERTs – basic work

2005:
Stocktaking

2006:
Setting up &
Cooperation

2007:
Support operation
Quality assurance

2008:
Good practice
on CERT
exercises

2009:
Pilot good
practice on
CERT
exercises

A STEP-BY-STEP APPROACH
ON HOW TO SET UP A CSIRT

Including examples and a checklist in form
of a project plan

CERT cooperation and its
further facilitation
by relevant stakeholders

A COLLECTION OF GOOD PRACTICE
FOR CERT QUALITY ASSURANCE

Deliverable WP2007/2.4.9 (CERT-D3)

E-CoAT

NCIRC
NATO
COMPUTER INCIDENT
RESPONSE CAPABILITY

FIRST
Improving Security Together

TRUSTED
Introducer

APCERT
Asia Pacific Computer Emergency Response Team

[…]

CERTs in Europe

CERTs in Europe map 2007 v1.5 © European Network and Information Security Agency (ENISA)

CERTs as "digital fire brigade"

Governmental CERTs in Europe 2005

Governmental CERTs in Europe 2008
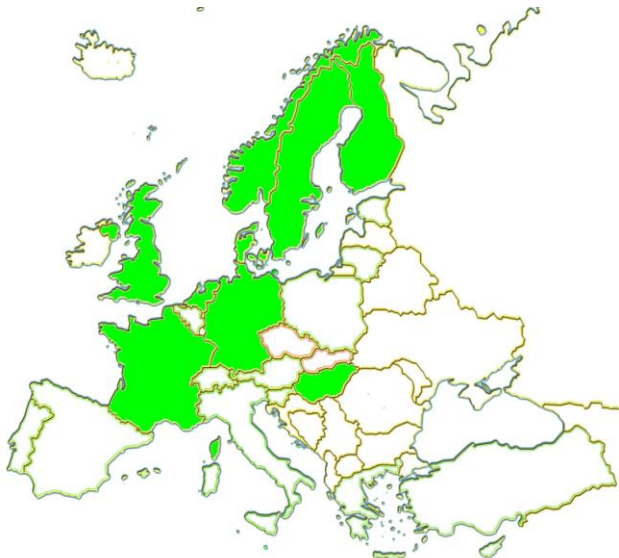
UK   Norway
The Netherlands   Sweden
Germany   Finland
Hungary
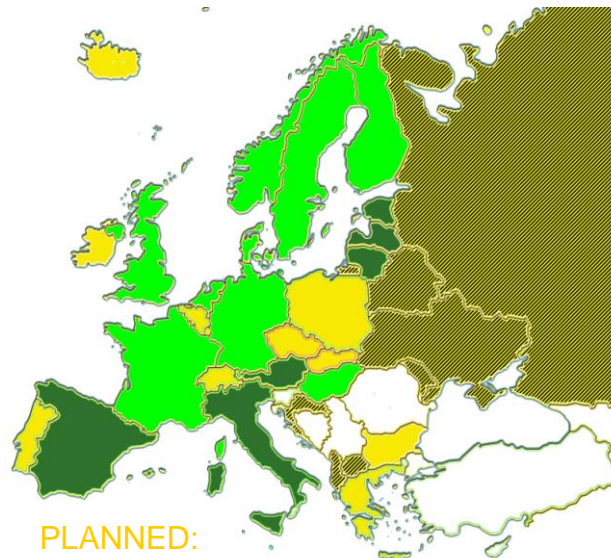
PLUS: PLANNED:
Spain   Portugal   Poland
Italy   Iceland   Slovakia
Austria   Ireland   Bulgaria
Estonia   Belgium   Greece
Latvia   Czech Rep.   Czech Rep.
Lithuania   Lithuania   Lithuania

Outside EU:
Most former Soviet Republics

+ Russia

ENISA helping to address SMEs
Is an EU-wide info sharing & alert system (EISAS) feasible?

EISAS – European Information Sharing and Alert System

A Feasibility Study
2006/2007
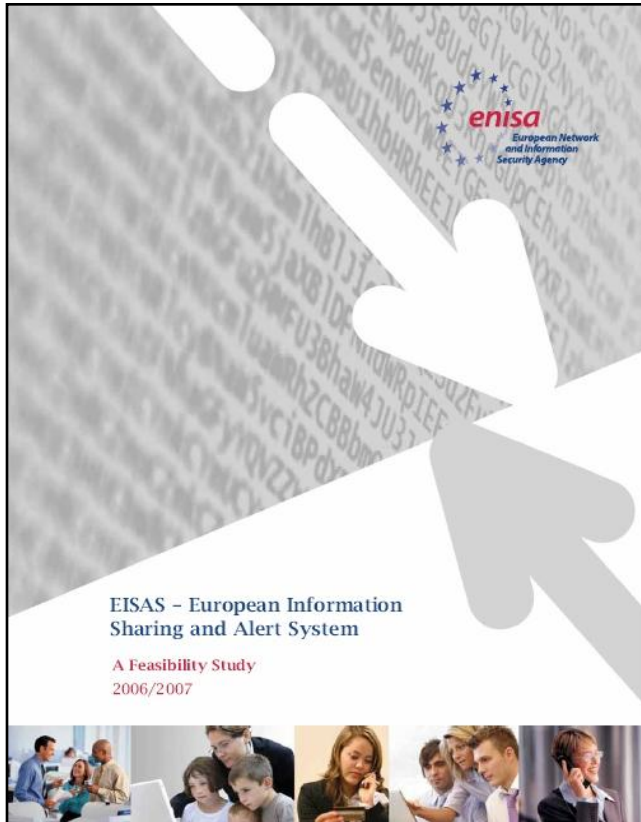
Feasibility study (COM request 2007)
Focussed on home users and SMEs

Most feasible scenario builds on existing national ISASs

EU as facilitator of good practice for national ISASs (no operational role for EU)
Clearing house for new ISAS
Support new ISAS
Facilitate dialogue between existing ISAS
Analyse and review methods of ISAS

Follow-up by DG JLS
Call for proposals April 2008
http://ec.europa.eu/justice_home/funding/cips/doc/call_2008_en.pdf

Imbalance in Member States' capabilities
Some more "equipped" than others?

Limited number of MS already work together to exchange experiences in order to develop their NIS capabilities

All MS should support each other by sharing information and lessons learned on good practices on a structural basis
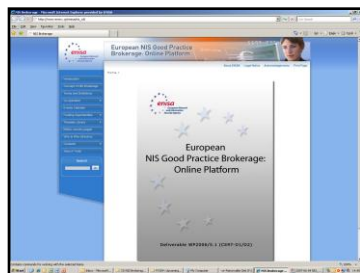
ENISA acts as broker between MS

The ENISA team
at your service

Member States working together

The PSG members
are willing to share

Online Platform
as supporting tool

ENISA Brokerage in action
Some cases

Hungary supporting Bulgaria in setting up governmental CERT

Finland willing to support Slovenia in organising awareness raising activities

Netherlands and Hungary envisage cooperation in structured cyber crime-related information exchange, to be expanded to other countries

MTP 3 – emerging risks

★ Framework for assessing and discussing emerging risks

★ Position Papers

Success stories

* Follow the major and emerging technological developments trends
* Position Papers on
    * Botnets
    * Security Issues for Reputation-based System
    Der Spiegel, Le Monde, Harald Tribune, Computer Weekly, ...
* Online inventory of RM tools&methods
* RM Information Package for SMEs
* Inventory of NIS Standards (collaborative project with ITU
* Response to requests

★ WPK 4.1: WG - Analysing micro enterprises' needs and expectations

★ WPK 4.2: Assessing risk management process for micro enterprises

How does ENISA engage stakeholders?
Bringing them together: "NIS is people"

ENISA Bodies
Management Board
Permanent Stakeholders' Group
National Liaison Officers network

Expert groups
Ad-hoc Working Groups
Virtual Expert Groups
Consultation workshops

EU Institutions
European Parliament, Council, COM

Multiplier organisations
Road show to industry, users/consumer

Communication and outreach
Website
ENISA Quarterly Magazine
Conferences and Joint Events
Dissemination workshops

How can you cooperate with ENISA?

★ **Be an** expert collaborating with ENISA in NIS Experts Pool database

★ Participate in one of ENISA's current and future Virtual Expert Groups

★ Make (pilot) use of our Results and Studies, e.g.,
  - ★ A User's Guide on How to Raise NIS Awareness
  - ★ Step-by-step Guide to setup a CERT
  - ★ Risk Management Information Package for SMEs
  - ★ Online inventory of Risk Management Tools & Methods
  - ★ ISP Measures on Security and Anti-Spam

★ Help to draft ENISA's Position papers

www.enisa.europa.eu

How can you cooperate with ENISA?

★ Send a specific Request or a Call for Assistance (Applicable for EU and Member State's competent bodies)

★ Participate at ENISA's dissemination workshops

★ Call ENISA to Support/Co-organise Jointly Events (Conferences, Workshops)

★ Write an article about your activities for our magazine "ENISA Quarterly Review" to outreach a wide expert audience in the EU (>10000 downloads per issue)

Stay in touch with ENISA!

Visit our web pages:

Subscribe to our Quarterly Review Magazine:

www.enisa.europa.eu