



# ENISA comments on ARECI study

Stakeholder meeting – Brussels 18 June 2007

Alain Esterle

Head of Technical Department

[Alain.esterle@enisa.europa.eu](mailto:Alain.esterle@enisa.europa.eu)

Mehis Hakkaja

Expert – Computer Incident and Response Handling

[mehis.hakkaja@enisa.europa.eu](mailto:mehis.hakkaja@enisa.europa.eu)

Simone Balboni

Seconded National Expert – Risk Management

[simone.balboni@enisa.europa.eu](mailto:simone.balboni@enisa.europa.eu)



# Structure of ENISA comments

- 10 comments for 10 recommendations;
- 1 comment for Key findings;



Heraklion, 3<sup>rd</sup> May, 2007

## ENISA comments on the EC study on availability and robustness of electronic communication infrastructure

### 1 Context

ENISA received a request (see email in Annex A) to comment on a study on availability and robustness of electronic communication infrastructure. The deadline to receive comments is 18<sup>th</sup> May.

In this document, ENISA expresses its point of view on the recommendations presented in this study.

The study is available here:

[http://ec.europa.eu/information\\_society/newsroom/cf/itemdetail.cfm?item\\_id=3334](http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=3334)

A general comment on the study is that it describes problems but does not suggest detailed solutions. ENISA agrees in general with the suggested recommendations, but would like to make the following comments. ENISA would also like to suggest two other recommendations.

### 2 ENISA comments

#### Recommendation 4.1

This recommendation is very important, and to some extent self-evident in a study on availability of critical infrastructure, because it's a central concept of all Business Continuity Management methods. It should also be noted that joint emergency exercises are just one phase in a more complete Risk Management framework that comprises a deep analysis of the system with the interconnections between

General comment:

**ENISA agrees in general with the suggested recommendations.  
The study describes well the problems, the suggested solutions are not detailed.**

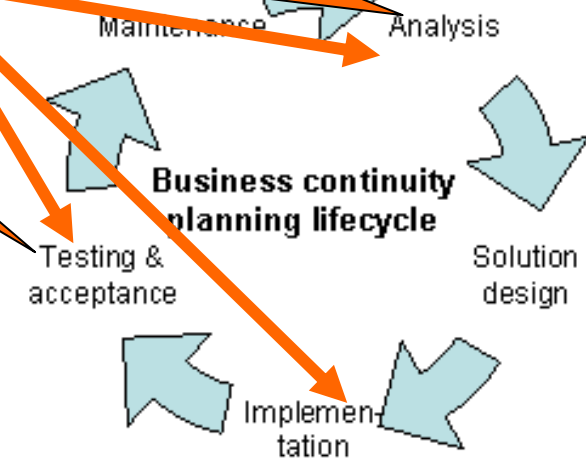
# #1 More structured RM approach

R1: Emergency Preparedness

R5: Inter-Infrastructure Dependency

R3: Mutual aid agreements

to be merged in a more structured  
**RISK MANAGEMENT APPROACH**



Foster research on:


- RMRA methods to address large dependable systems
- governance of e-communication systems





## R6: Supply Chain Integrity and Trusted Operation

1. asset oriented approach to identify asset specific security levels
2. no mention of the public discussion on Trusted Computing (FLOSS, DRM and the delicate role of EU and MS)

Relevant IST Links

 [Print friendly](#)

IST Results 



# IST Results

What is IST Results

News & Features

Press Desk

Investors Room

Help & Links

## FLOSSing can make EU tech leader



The Information Society is on the cusp of a seismic shift in the creation, and even the business of its key enablers. Europe is in an excellent position to take advantage of that shift through an emphasis on Open Source Software.

The [CALIBRE](#) project seeks to bolster that position by creating a network of experts in Free, Libre, and Open Source Software (FLOSS), rapid software development, and Global Software Development (GSD), where pieces of an application are developed at different locations.

Market emphasis is shifting from primary software companies like Microsoft, Oracle and SAP, Europe's primary software developers to secondary software developers like Nokia, Philips, Daimler-Chrysler and Siemens. Secondary developers create software as an end in itself.

"There's probably more secondary software out there than there is primary. It's in more devices, like cars and phones and other consumer electronics," says Prof. Fitzgerald, at the University of Limerick, and coordinator of the IST-funded CALIBRE project.

Prof Fitzgerald says that Europe is the world leader in secondary development, while the US leads in primary development, a market that is growing rapidly.

"While secondary software is everywhere, it is not so obvious. It's hidden from the user. But in a not-too-distant future all software will be secondary software; they'll simply use them like any other utility such as gas or electricity. They'll only pay for what they use, while primary software is as long as it gets the job done," says Fitzgerald.

"Instead of developing a whole system, which is costly and expensive, in the open source model SMEs can cheaply develop extensive value-added services that they can charge for," says Fitzgerald.

The major hiccup to this open source software development model is that, currently, there is too little awareness of FLOSS potential. There is an inherent prejudice against FLOSS. Many policymakers and businesses believe that if the underlying software is free, it can't be good. In fact, open source techniques can actually create more reliable, efficient and secure software than traditional methods, working on the principle that many eyes make all bugs shallow.

# #3 Standardization

Password:



5599 7774



## R7: Unified European Voice in Standards

It is stressed the need for a direct participation of MS in standardisation.

→ we think industry remains the leading driver of standardisation

Main stress on a role for EU&MS to foster:

- cooperation between industry and MS e.g. in the preparatory activities, requirements capture phase, planning, gap analysis
- information sharing and involvement of all stakeholders (ICT Security Standard Roadmap portal by ENISA/ITU/NISSG)

# #3 Standardization/2

Password:

5599 7774



<http://www.itu.int/ITU-T/studygroups/com17/ict/>



ICT Security Standards Roadmap  
(Version 2.0, May 2007) -- Select a Part of the Roadmap --



[Part 1: ICT Standards Development Organizations and Their Work](#)

[Part 2: Approved ICT Security Standards](#)

[Part 3: Security standards under development](#)

[Part 4: Future needs and proposed new security standards](#)

[Part 5: Best practices](#)



## R2: Priority Communications on Public Networks

ENISA agrees with the **urgency** of this recommendation:

achieving priority on future networks will be more challenging

→ opportunity to do it from the very beginning

- EU & MS to work with Standardization Bodies to collect requirements
- EU & MS to fund research on PC models → powerful driver to have them on next generation networks



## R4: Critical Infrastructure Information Sharing

Private Sector Service Providers and Government Authorities "must be willing to share information for the common good".

→ major aspect missing: **motivation**



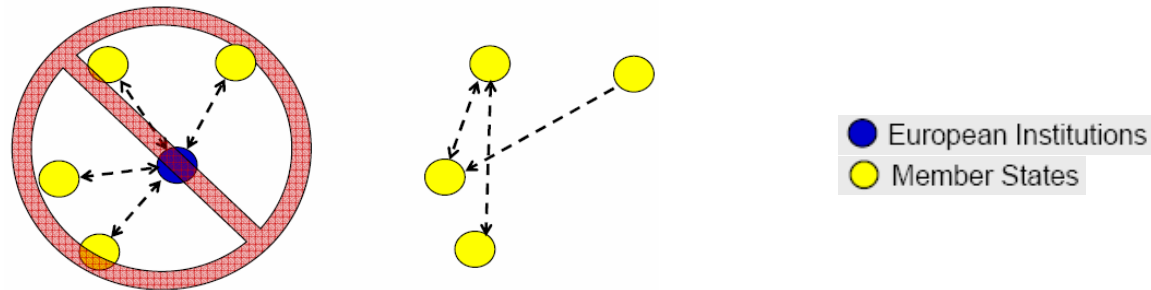
monetary or regulatory



## R4: Critical Infrastructure Information Sharing/2

Star topology not appropriate **but** we do believe that an element of European coordination is necessary.

“Next Steps” discuss information sharing only within or between MS, but do not mention how this would be coordinated in Europe.



ENISA is working on information sharing within two projects as requested by the European Commission:

1. Examining the feasibility of a data collection framework;
2. Examining the feasibility of an EU-wide information sharing and alert system. [www.enisa.europa.eu](http://www.enisa.europa.eu)



## R8: Interoperability Testing

Presence of SME's and measures to guarantee an open governance for the envisaged N2N testing framework

## R9: Vigorous Ownership of Partnering Health

Motivation of partners to work together → **why and how**  
“Partnering Health” misleading

## R10: European Expert Best Practices

More details of how EU&MS could encourage the use of Best Practices  
(Repository - Incentives because of the implementation costs? Create a catalog? Fostering research?)