Deloitte.

Resilience of public eCommunications networks:

Analysis of policies, legal environment & country practices.

ENISA Workshop on resilience

Brussels, Belgium

November 12, 2008

Audit . Accounting . Tax . Consulting . Corporate Finance .

Structure of presentation

A. Introduction

B. Approach

C. A snapshot of key findings

D. The way forward

A. Introduction

A. Overview

- The project focuses on resilience of public e-communications (eComm) networks
- The purpose of the project is to produce a qualitative analysis of data collected for each country in-scope through the stock taking exercise
- This analysis identifies commonalities and differences among MS' activities for each Topic
- Also, it outlines and assesses the MS' input on groups of topics ("super-topics").
- Finally, our analysis will provide a summary of findings and a set of recommendations for consideration.

A. Countries covered by analysis

EU Countries not covered:

- Austria
- Italy
- Malta
- Slovakia
- Romania

A. The project tackles a “vital” resource

The key findings of our analysis confirm as common belief of the in-scope countries that:

- eComm networks and services represent a key driver of today’s business, economy and welfare;
- Disruptions/accidents of eComm networks or security incidents affecting them can have devastating effects to business and everyday citizens’ life;
- Today, the “preparedness” measures to ensure the resilience of eComm networks are tackled from different angles, and in different manners by countries;
- There is currently no clear direction at EU level on policies and measures regarding the security & resilience of eComs networks.

A. Project Challenges

- The countries in scope do not necessarily share the same understanding around several areas:
  - Resilience (Physical infrastructure? IT security? Protection of data?);
  - e-communications public networks (“essential” networks?);
  - “National risk management” (threat assessment? crisis response?).
- Empirical findings vary in terms of level of detail, clarity and accuracy of responses.
- Useful extrapolations from the “AS IS” situation to “TO BE” situation are provided in some country reports.
- Project aims to bring upfront “good” practices and “case scenarios” as:

– a “learning tool” for less advanced countries;

– a “trigger” to identify opportunities for a more harmonized approach IF wished IF necessary.

B. Approach

B. Approach

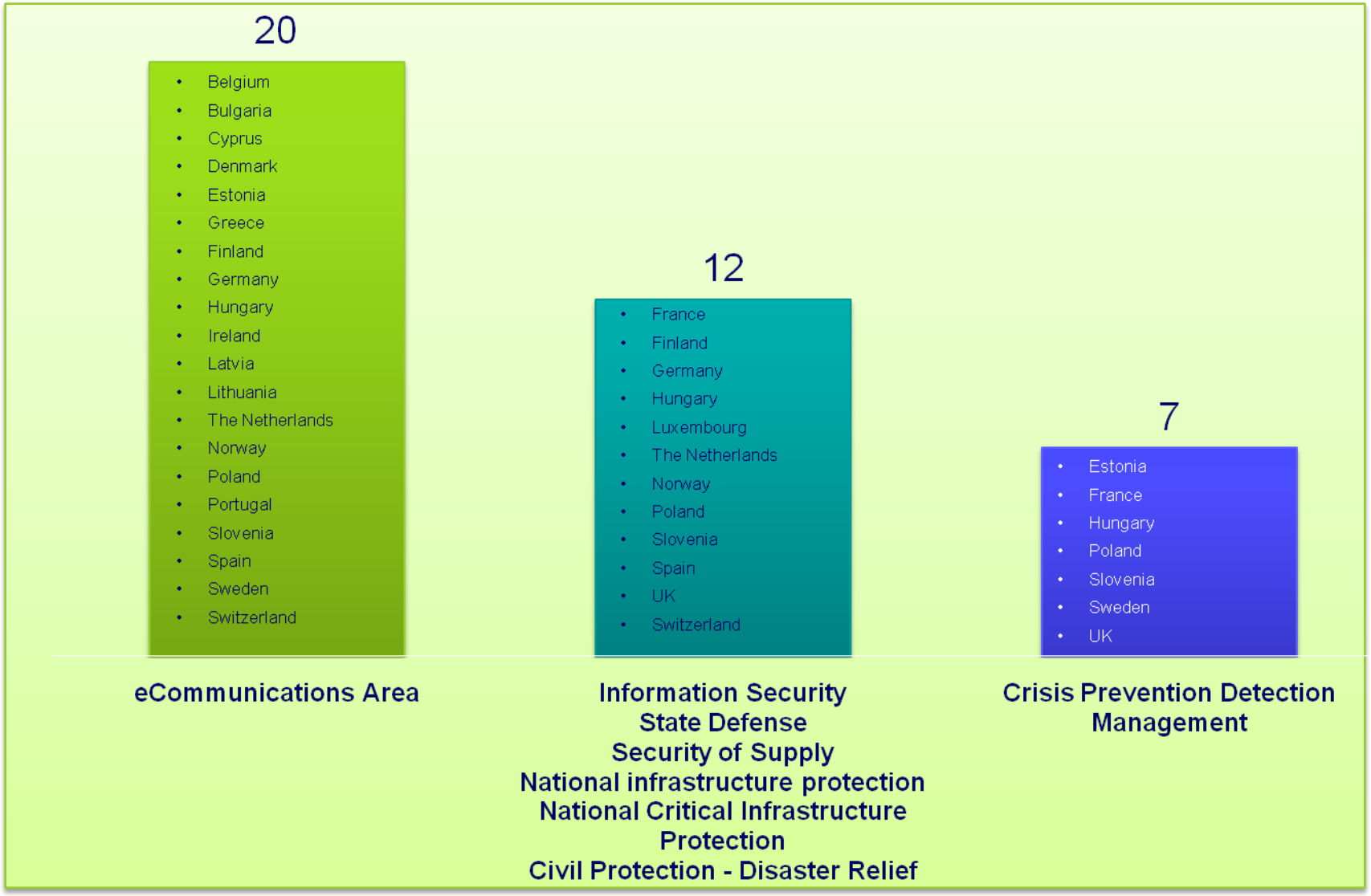
- Our analysis will be documented in a formal report.
- We structured our analysis as follows:
  - Starting point: analysis of country survey responses per “Topic” (14 questions/topics);
  - Identification of “super-Topics” – topics that transcend one individual area;
  - Identification of good practices at country level that could be highlighted and shared:
    - done per “cross-Topic”,
    - as an overview of concrete case scenarios “tested” in the practice of certain countries, for your consideration.
  - Recommendations:
    - Where should the accent be put to enhance resilience?
    - By which actors (countries, ENISA, EU...)?

C. A snapshot of key findings

C. The “super-Topics”

- The “Governance Model” of resilience
  - Competent Authorities
  - Mandate, responsibilities & tasks
  - Regulatory framework, procurement practices
- Initiatives and cooperation
  - Good practices, incentives
  - Initiatives (e.g. PPP, working groups, best practice repositories)
- National risk management and preparedness
  - Risk Assessment
    - Information Exchange (nature, form, frequency, results)
    - Incident reporting
    - Incident Reporting Capabilities
  - Risk Mitigation
    - Preparedness measures
    - Audits, exercises
    - Enforcement actions

C. Insight: Competent authorities



C. Insight: Regulatory framework

- Network resilience “touches” a variety of areas of law, which complicates the identification of requirements.
- A “principle-based” approach to resilience gained room in a number of countries:
  - e.g. Netherlands, Ireland, Spain.
- Co-regulation seems to be a good compromise between “strict law” and “self-regulation” for a few countries:
  - e.g. Germany, Sweden.
- Market initiatives come to fill-in the regulatory gap in a number of countries:
  - e.g. Cyprus, Hungary.
- National regulation in a number of countries focuses mostly on “reactive” measures rather than preparedness measures:
  - e.g. Belgium, Hungary, Ireland, etc.

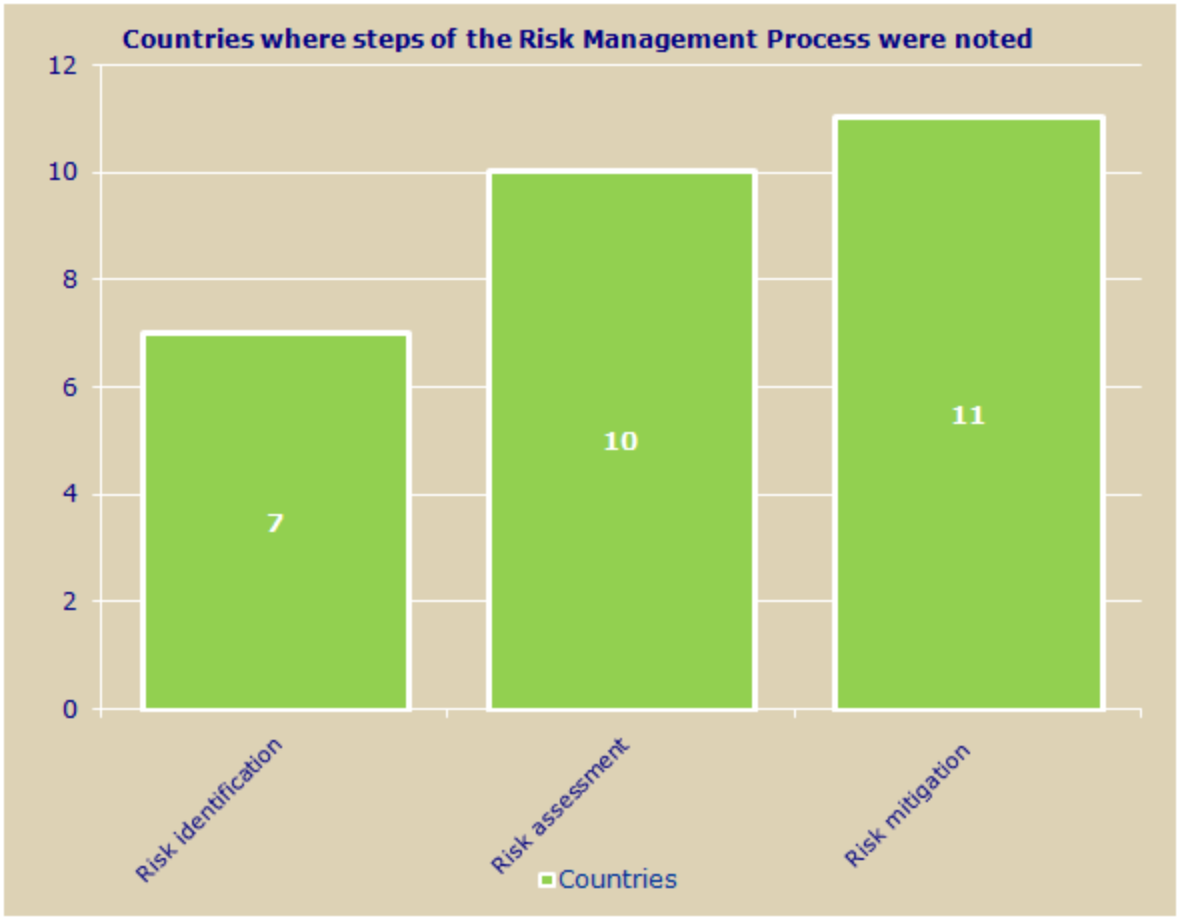
C. Insight: Initiatives & cooperation

Current models of information sharing and cooperation reflect following tendencies in the countries in scope:

- The “need to know” approach: operators provide information to authorities if and when they are asked:
  - e.g. Belgium, Cyprus, Denmark, Greece;
- The “have to know” approach: mandatory communication of information, especially in case of security incidents;
- More pronounced cooperation, “public-private” models taking various forms, such as:
  - Finland: National Emergency Supply Council (NESC)
  - Germany: CIP Implementation Plan
  - Ireland: concept of ‘structured exercises’
  - UK: Electronic Communications Resilience and Response Group (EC-RRG)

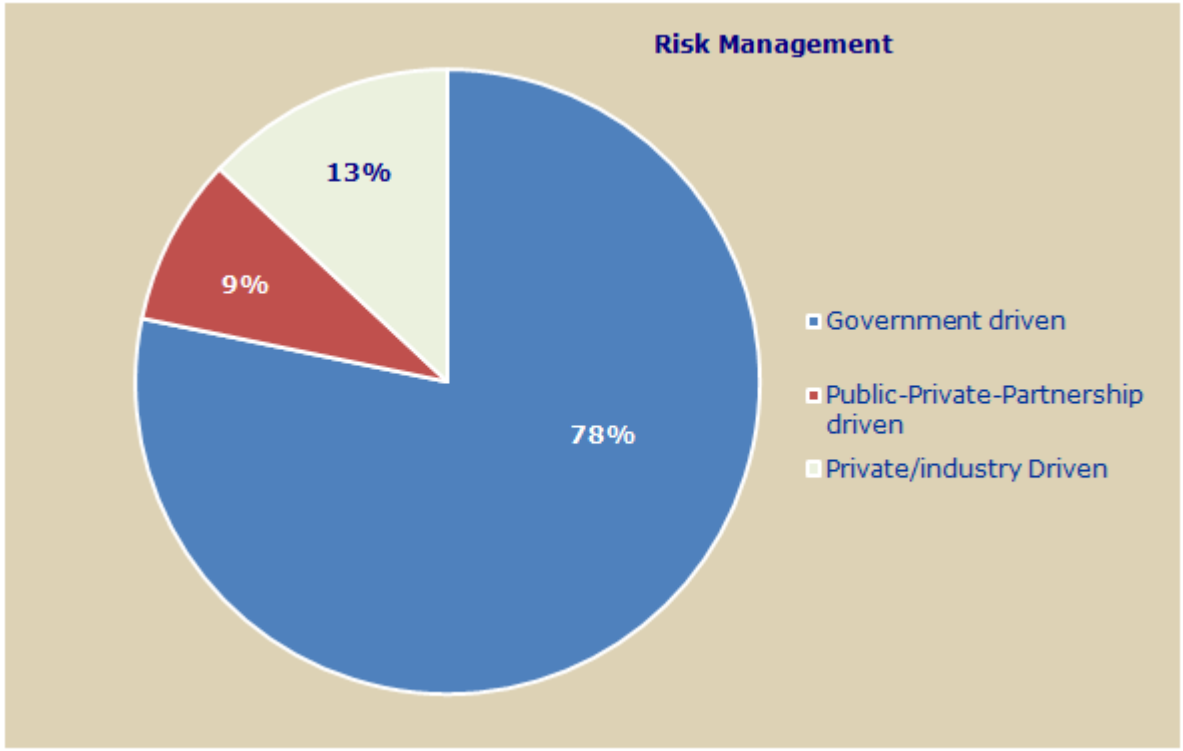
C. Insight: National Risk Management Process

- Out of 24 countries covered, only several have identified as such the steps of the risk management process:

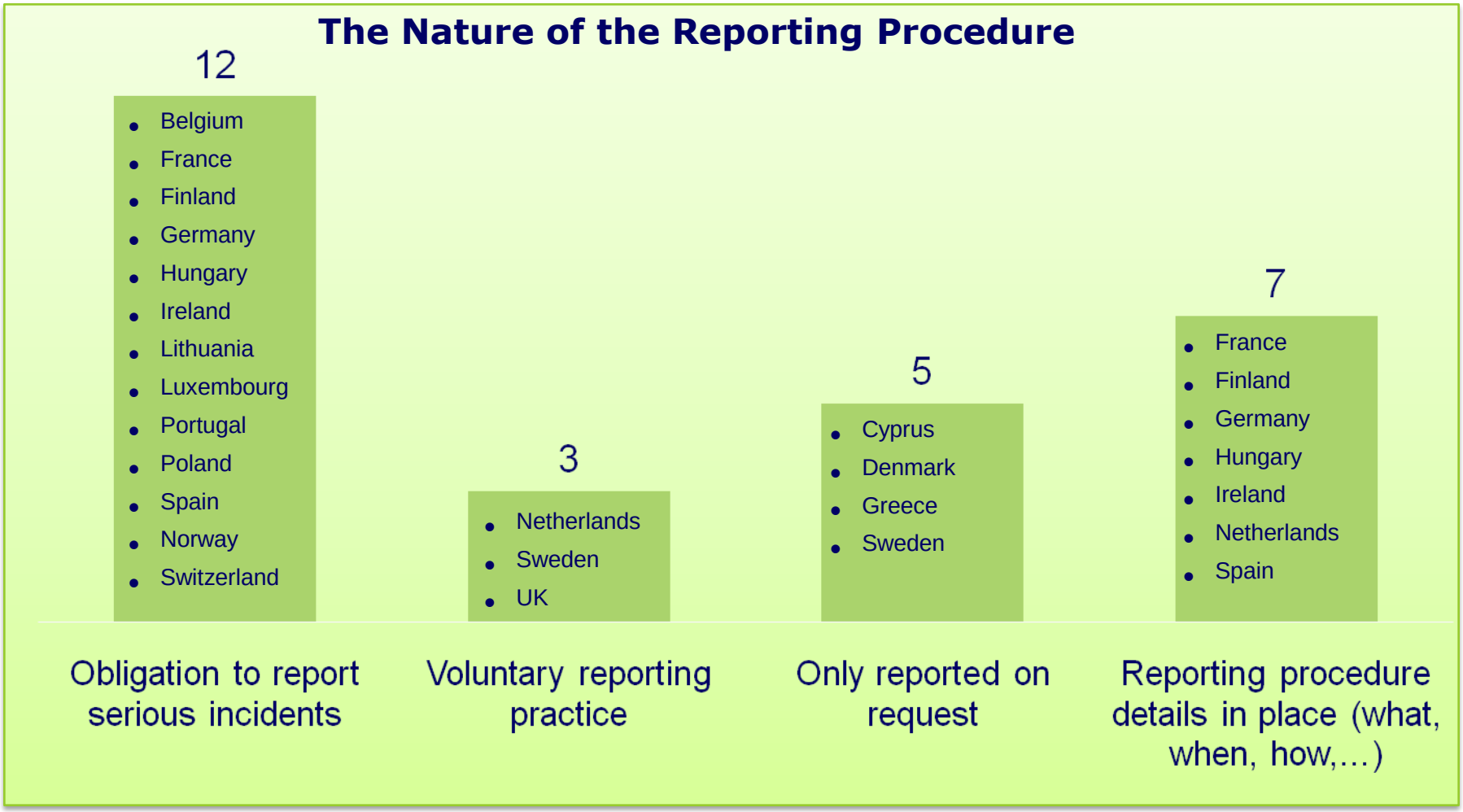


C. Insight: National Risk Management Process (cont'd)

- In the majority of the countries, risk management process related to the resilience of public and/or other essential eComm networks is driven by the government



C. Insight: Incident Reporting (1)



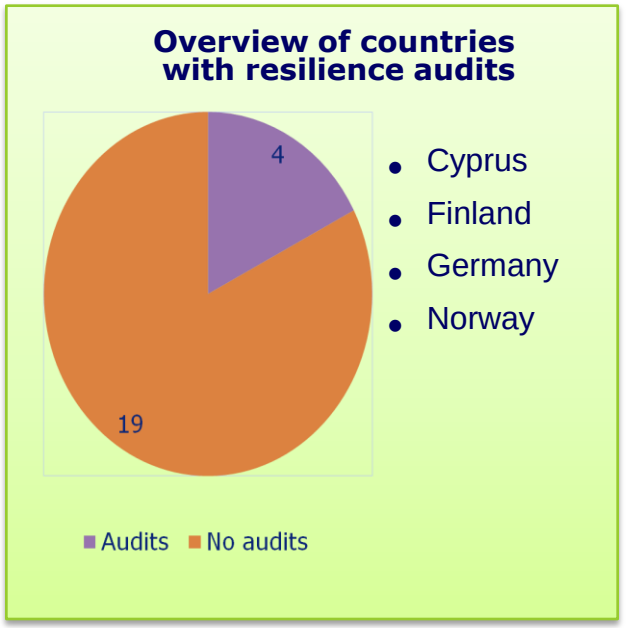
- Many countries imposed reporting of security eComm resilience incidents.
- When reports are to be made, procedures guiding the reporting process are not always in place or not always detailed.

C. Insight: Incident Reporting (2)

- In many countries incidents become known through media and press!
- Definition of “serious” incidents and their scalability differs between countries (if any):
  - France: major/minor failures defined in the law;
  - Norway: >10.000 subscribers or an area larger than a municipality affected and lasting for more than 5 hours;
  - Spain: >100.000 citizens;
  - Switzerland: > 50.000 inhabitants.
- Good practice example:
  - Sweden: direct involvement of users in incident reporting and follow-up with operators.

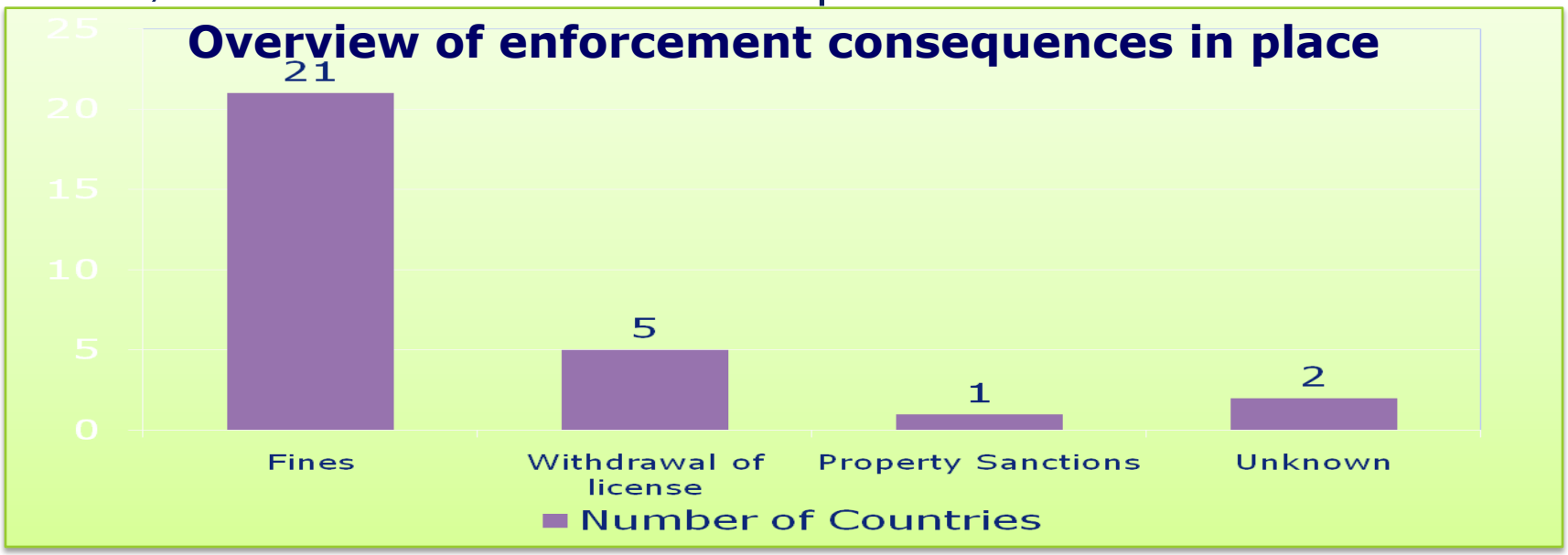
C. Insight: Audits

- The majority of countries consider audit as an exceptional tool in their risk management and risk mitigation procedures.
- Resilience audits (if any) are performed:
  - By the regulatory authority,
  - On a regular basis and possibly after an incident.
- Easier adoption of softer approaches for control of compliance than on site investigations:
  - Submission of mandatory information to authority:
    - "Security Concepts" (Germany),
    - "Security Master Plan" (France),
    - Summary of "recovery plans" or of Business Continuity Plans (Spain);
  - Conduct of "desk" or "testing" exercises with operators (Netherlands, Ireland)

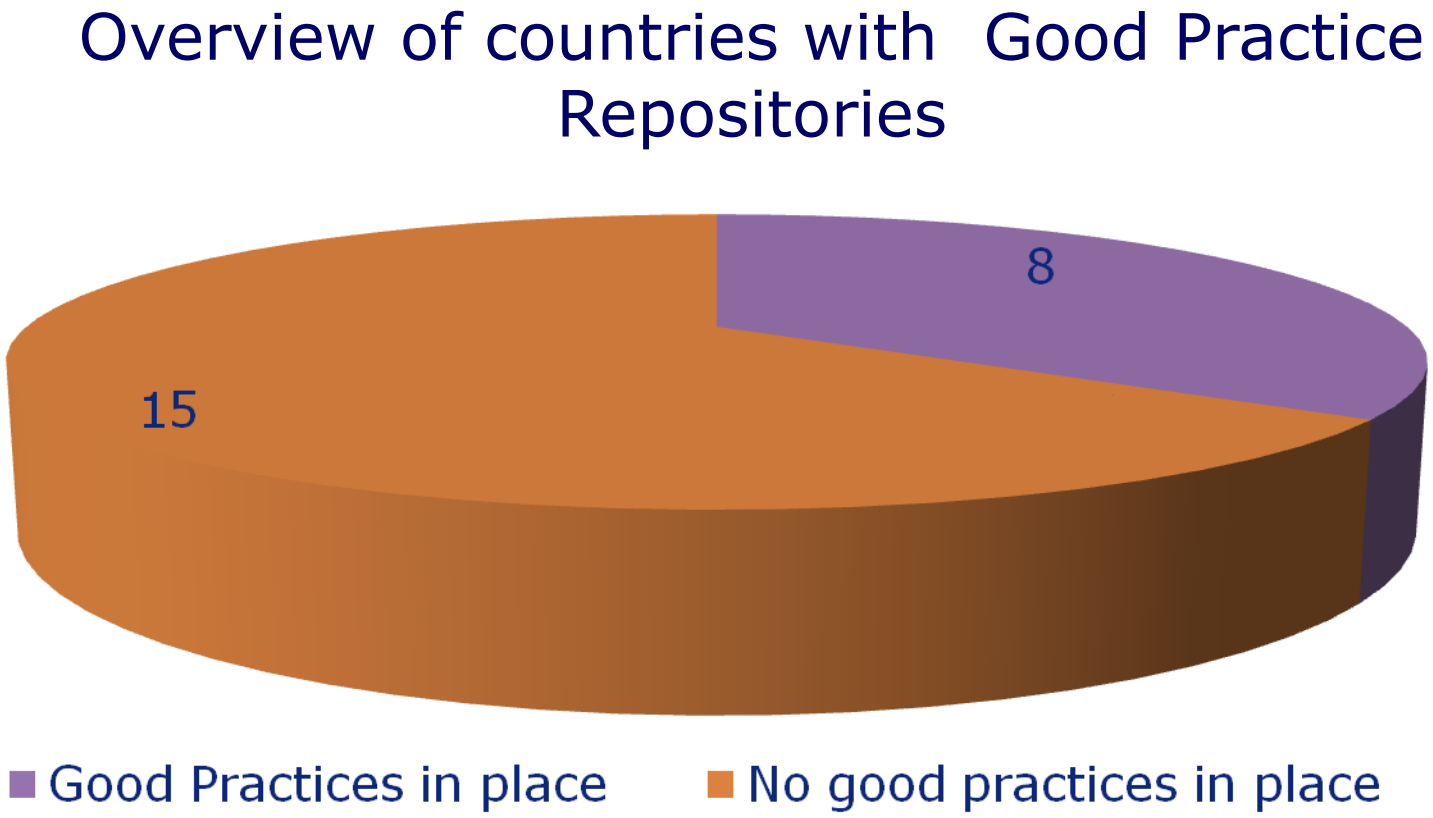


C. Insight: Enforcement

- There is a general tendency in all countries to settle the problem if an incident happens rather than to punish.
- No country reported any specific enforcement action taken towards operators who infringed resilience rules.
- In several countries, the legislation on resilience is in general terms, which makes enforcement problematic.



Insight: Good Practice Repositories



D. The Way Forward

D. Results & timelines

- Analysis report submitted to ENISA: mid-end of December 2008.
- Opening of public consultation: mid-January 2009
- Stakeholders' feedback and comments: beginning-mid February 2009
- Final Analysis report accommodating YOUR comments submitted and published: mid-end February 2009.

Any Questions?

- **Georgia Skouma**

  Project Manager, Deloitte

  – Tel: +32 2 800 24 93

  – Email: gskouma@deloitte.com