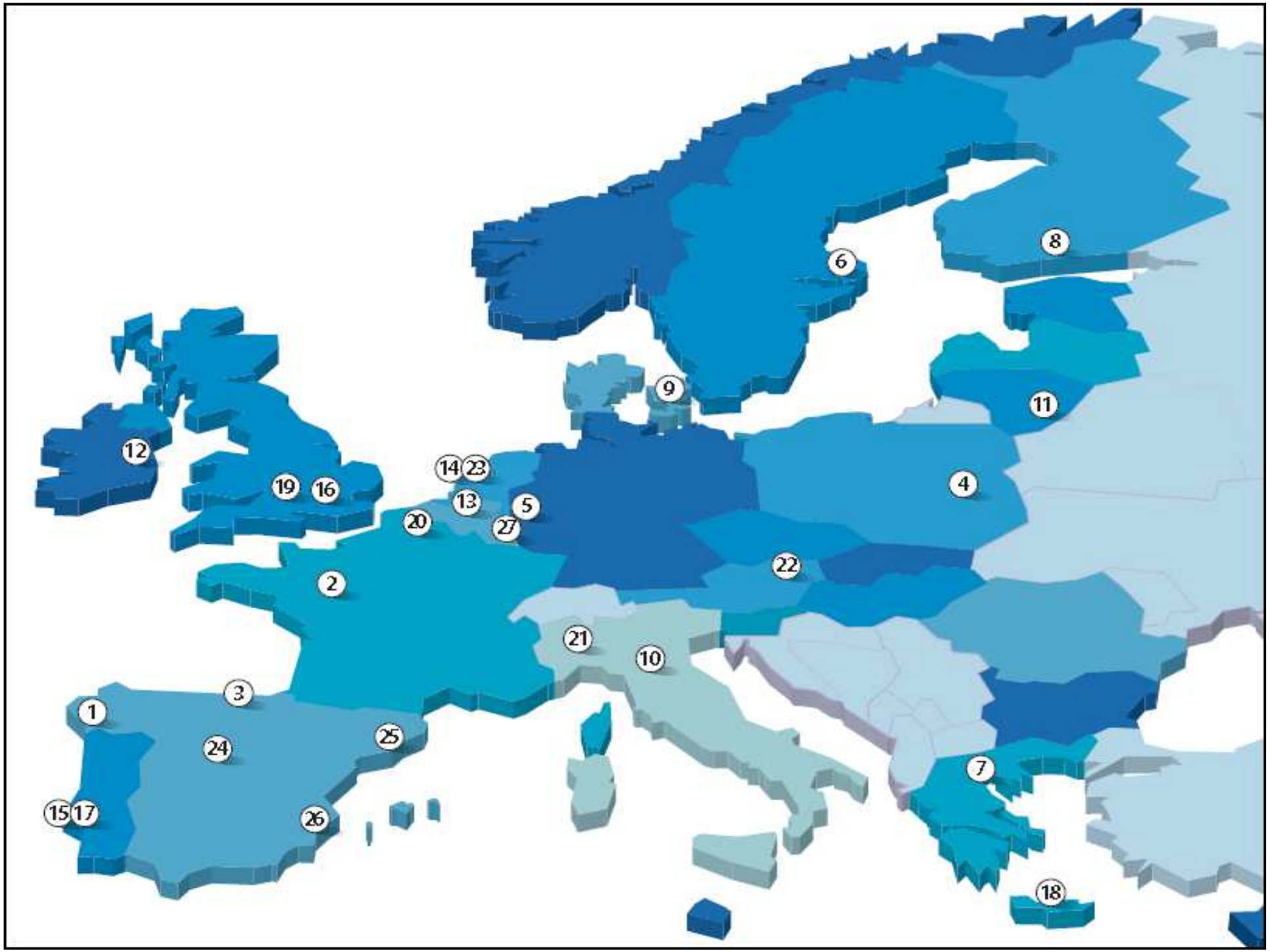
# Preventing and reporting about security and integrity breaches

Implementing Article 13a of the EU telecom reform

Marnix Dekker, ENISA


8
6
9
11
12
14
23
4
19
16
13
5
20
27
22
2
21
10
3
1
25
24
7
15
17
26
18


communications
states
member
networks
measures
ensure
undertakings
national
integrity
accordance
providing
take
technical
inform
regulatory
security
authority
concerned
available
taken
european
publicly
requirements
implementing
prevent
may
appropriate
public
services
electronic
paragraphs
breach
impact
enisa
commission
referred
article
supplementing
circumstances
disclosure
taking
submit
action
greatest
operation
directive
information
designed
additional
regard
risks
supply
defining
continuity
agency
network
appropriately
provided
report
incidents
non-essential
harmonising
minimise
international
steps
determines
account
manage
competent
procedures
posed
interconnected
pursue
require
adopting
authorities
based
year
paragraph
format
elements
interest
users
particular
view
objectives
order
opinion
utmost
standards
extent
adopted
risk
amend
significant
notification
guarantee
notifications
thus
possible
13a
22
presented
received
notify
level
applicable
procedure
set
summary
adopt
state
loss
including
organisational
scrutiny

# Article 13 summary

- Appropriate security measures
  - to minimize impact of security incidents on users and interconnected networks
  - to guarantee network integrity, thus ensuring continuous supply of service over the networks
- Incident reporting
  - Telcos report significant incidents to their NRA
  - NRA's inform other NRA's abroad and ENISA when appropriate
  - NRA's can inform the public when this is in the public interest
  - NRA's provide an annual summary to ENISA and the EC
- Implementation and enforcement
  - NRA's can require information to assess security and integrity
  - NRA's can require telco's to submit to a security audit

# Article 13a WG

- ENISA (supporting role, expert advise)
- EC (observer)
- NRAs
  - PTS (SE), Ministry of Economic Affairs (NL), FICORA (FI), Ofcom (UK), ANACOM (PT), ComReg (IE), EETT (GR), ITST (DK), CPNI (UK), RTR (AT), ANCOM (RO), EA "ECNIS" (BG), ANSSI (FR), Bundesnetzagentur (DE), BIPT (BE), MITYC (ES), MPO (CZ), CERT LT (LT), MFSR(SK), ILR (LU), APEK (SI), MCA (MT), Ministry of Economic Development (IT), OCECPR (CY).
- Goals
  - Implement reporting scheme
  - Harmonized implementation across the EU

# Implementing Article 13a

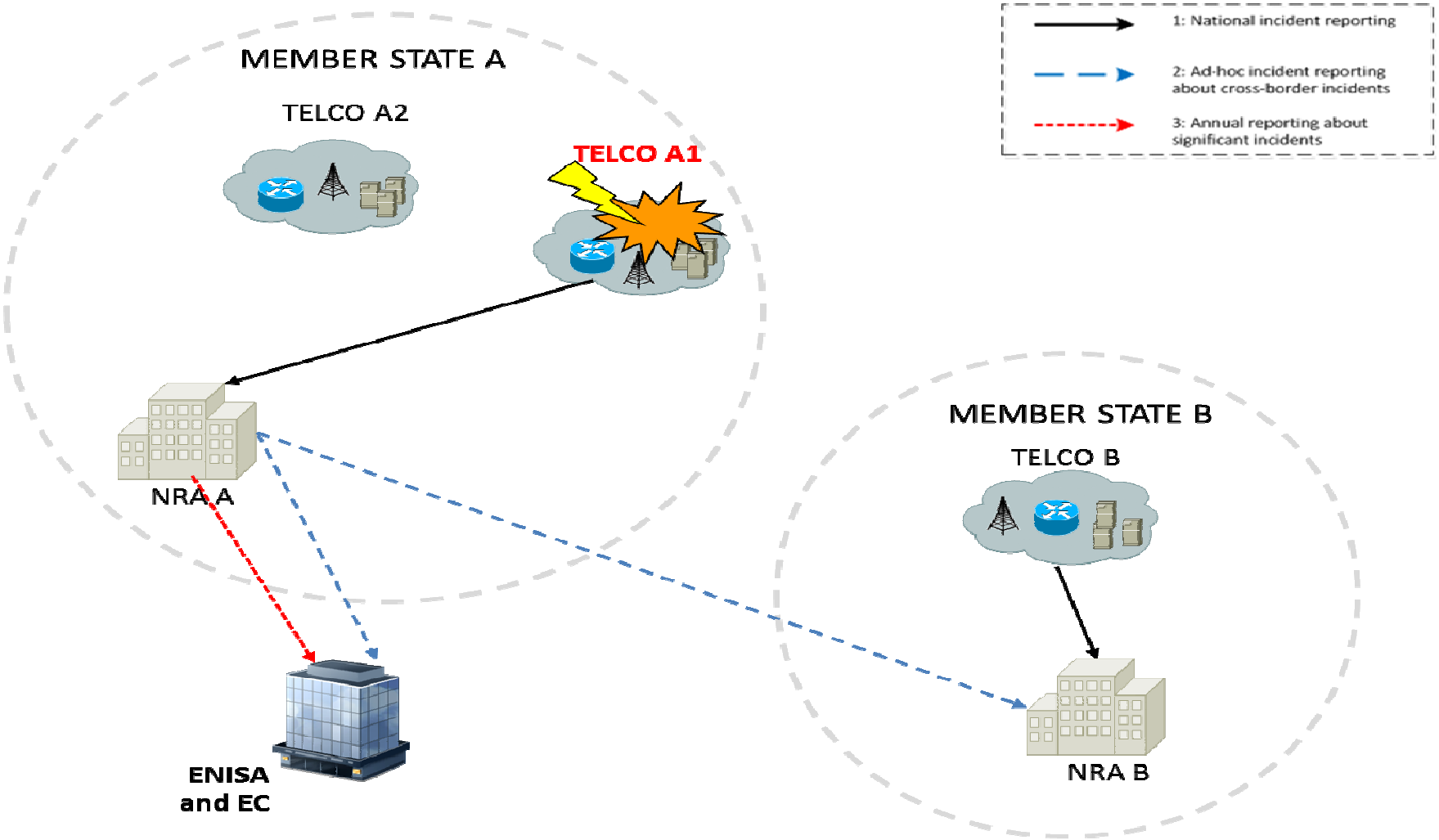
- Security and integrity
  - Integrity = network integrity, continuity
- Appropriate security measures to address risks for users and interconnections
- Incidents with significant impact
  - at the discretion of NRAs

# ENISA Technical guidelines

- Non-binding technical guidance for NRA's
- Consensus among the NRA's

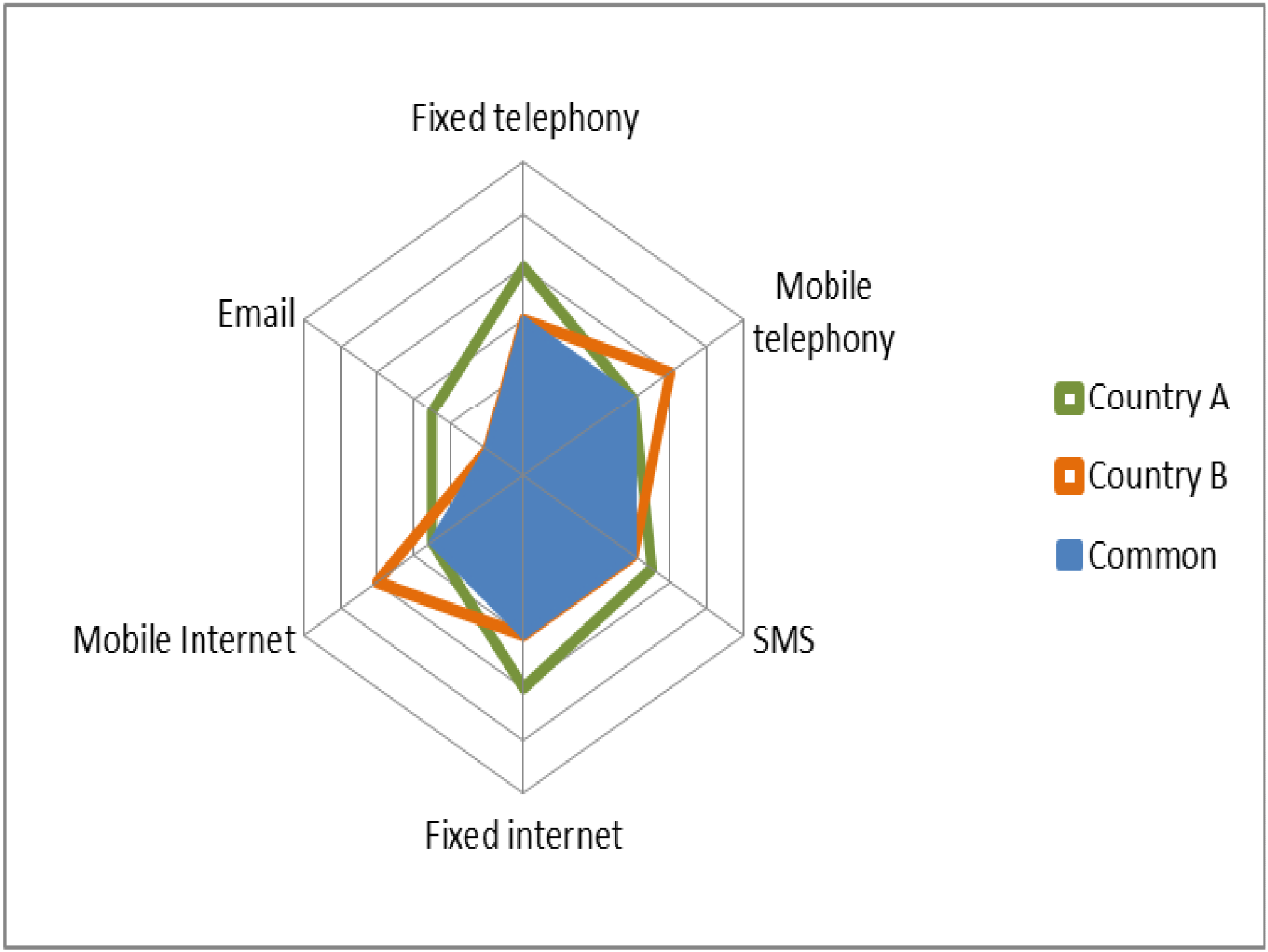

- Incident reporting
  - Thresholds for reporting
  - Rootcause classification
  - Reporting template
- Minimum security measures
  - 7 domains
  - ISO27K1 (subset) + BS25599 (for BCM and disaster recovery)

# Technical guideline for Incident reporting



# Preliminary scope annual reporting

- Incidents with a significant impact on the **continuity of supply** of electronic communications networks or services
- Services
  - Telephony
  - Internet
  - Messaging
  - Email
- Agreed set of incident parameters and thresholds


Fixed telephony
Mobile telephony
SMS
Fixed internet
Mobile Internet
Email
Country A
Country B
Common

# Thresholds for annual reporting

| | 1h<…<2h | 2h<…<4h | 4h<…<6h | 6h<…<8h | >8h |
|---|---|---|---|---|---|
| 1%<…< 2% of users | | | | | |
| 2% < …< 5% of users | | | | | |
| 5% <…< 10% of users | | | | | |
| 10% <…<15% of users | | | | | |
| > 15% of users | | | | | |

# Annual overview by ENISA

- Statistical analysis of incidents

- No comparison or information
  - about individual telcos
  - About individual member states

- Overall view of resilience and security of telecommunication networks and services

# Cross border incident

- ENISA received one report about a cross-border incident
- Power outage at a site in Scandinavia affecting all its subscribers in one country, and its subscribers in large areas of a neighbouring country.
- Rootcause: Faulty backup power
- Duration: >8 hours
- Users: Telco serves 10% of the total mobile subscribers.

| | 1h<…<2h | 2h<…<4h | 4h<…<6h | 6h<…<8h | >8h |
|---|---|---|---|---|---|
| 1%<…< 2% of users | | | | | |
| 2% < …< 5% of users | | | | | |
| 5% <…< 10% of users | | | | | |
| 10% <…<15% of users | | | | | |
| > 15% of users | | | | | |

# Technical guideline for Minimum Security Measures

- Risk assessment to determine the scope
- Domains
  - D1: Governance and risk management
  - D2: Human resources security
  - D3: Security of systems and facilities
  - D4: Operations management
  - D5: Incident management
  - D6: Business continuity management
  - D7: Monitoring, auditing and testing

# Example from the MSM guideline

The minimum security measures are grouped in domains (D1, D2 …) and in sub-domains (SD1.1, SD1.2, et cetera.

## D1: Governance and risk management

This domain covers the security measures related to (network and information security) governance and risk management.

### SD1.1 Information security policy

The Telco should establish and maintain an appropriate information security policy.

*Example: [from ISO27002 Ch 5] "Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organisation."*

### SD1.2 Governance and risk management framework

The Telco should establish and maintain an appropriate governance and risk management framework, to identify and address risks for the communications networks and services

# Example mapping to existing standards

| MSM | Telco | Compliance details |
|---|---|---|
| D1: Governance and risk management | ISO 27001/2 and ISO 27005 | ISO27005 describes methods for setting the scope of information security risk management. ISO27002 Ch 5 covers information security policy, governance, risk management and controls for third parties (who deliver services, hardware or software), such as security requirements and procurement procedures for developed or acquired information systems. |
| D2: Human resources security | ISO 27001/2 | ISO27001/2 Ch 8 covers security clearances, security roles and responsibilities, security knowledge and training, and personnel changes. |
| D3: Security of systems and facilities | ISO 27001/2 | ISO27001 Ch 9 covers the physical security of facilities, IT equipment and environmental controls |
| D4: Operations management | ISO 27001/2 | ISO27001 Ch 10 covers operational procedures, operational roles, classification, access control and change controls. |
| D5: Incident management | ISO 27001/2 | ISO27002 Ch 13 covers incident management. |
| D6: Business continuity management | BS 25999-1/2 | BS 25999 covers business continuity. |
| D7: Monitoring and security testing | ISO 27001/2 | Monitoring is covered in ISO27001/2 Ch 10; security testing and compliance monitoring and reporting are covered in ISO27001/2 Ch 15. |

# Current state of play

- 13 EU countries transposed (14 not, 12 almost)
- Half of the regulators will use ENISA guidelines
  - as advise to operators
  - to cross check compliance information
  - guidance for auditors
- Diverging approaches to incident reporting and security measures
  - Significant = >24 hours outage
  - Just a-posteriori investigation
  - Yearly submission of security templates

# Short term issues

- Incident reporting
  - First round of reporting
  - National incident reporting schemes
  - ENISA Reporting tool
  - Incident thresholds
- Minimum security measures
  - Staged approach
  - Compliance maturity
  - Audit guidance
  - Reference standards
- Relation with article 4 (personal data breaches)
- Extending Article 13a (internet security strategy)

Dr. Marnix Dekker, CISA
(marnix.dekker@enisa.europa.eu )
Resilience and CIIP at ENISA
resilience@enisa.europa.eu

The Article 13a WG portal:
https://resilience.enisa.europa.eu/article-13

Technical guidelines for Article 13a at
https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting
https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures