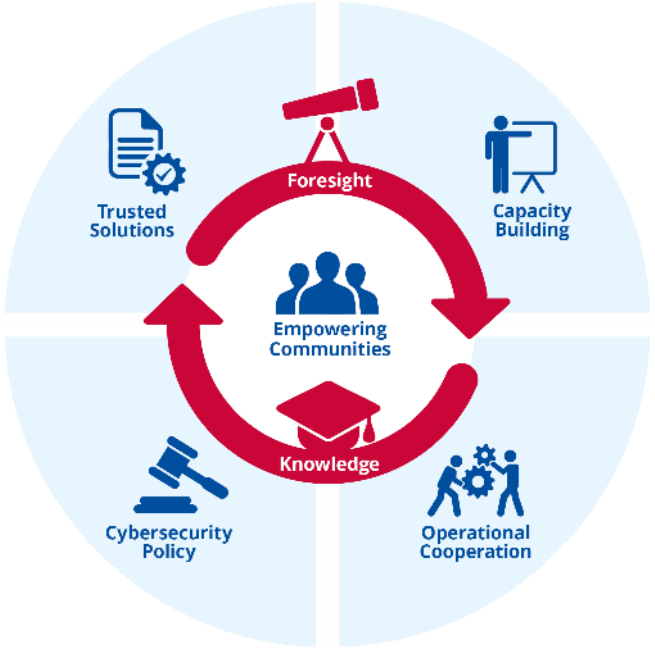
EUROPEAN UNION AGENCY
FOR CYBERSECURITY

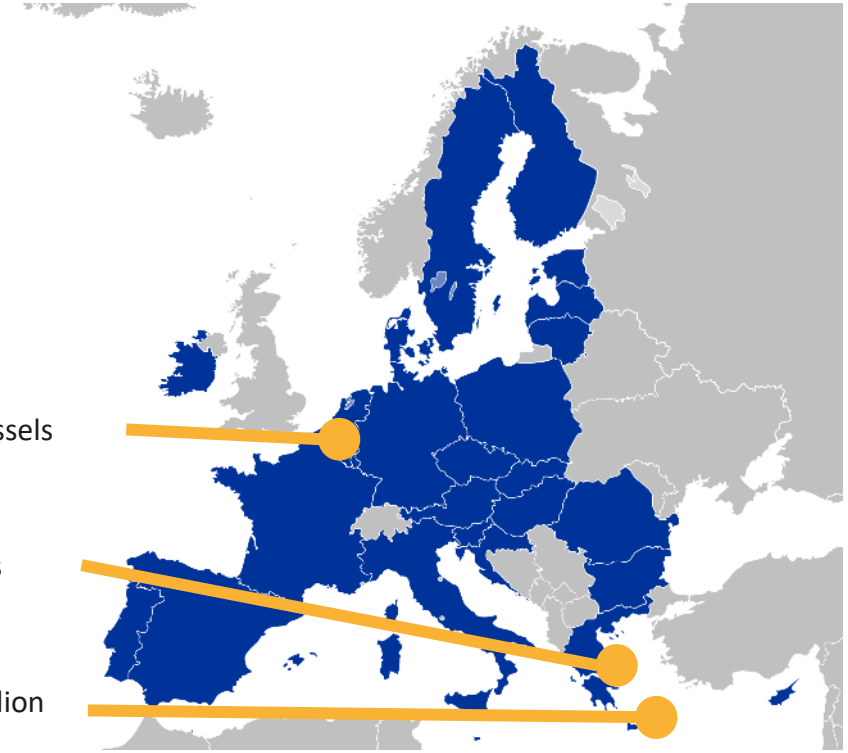
Cybersecurity for SMEs

3 | 10 | 2024

Evangelos Kantas – ENISA
Anna Sarri - ENISA
Awareness Raising & Education Team

ABOUT ENISA





About 150 staff - steadily growing

4 units doing cybersecurity work

- Operational collaboration (Cyclone, CSIRT network)
- Cyber exercises, challenges, trainings (Cyber Europe)
- Certification and standardization (EU schemes)
- Policy unit (including EECC, eIDAS, NISD, 5G, eID wallets, critical sectors)

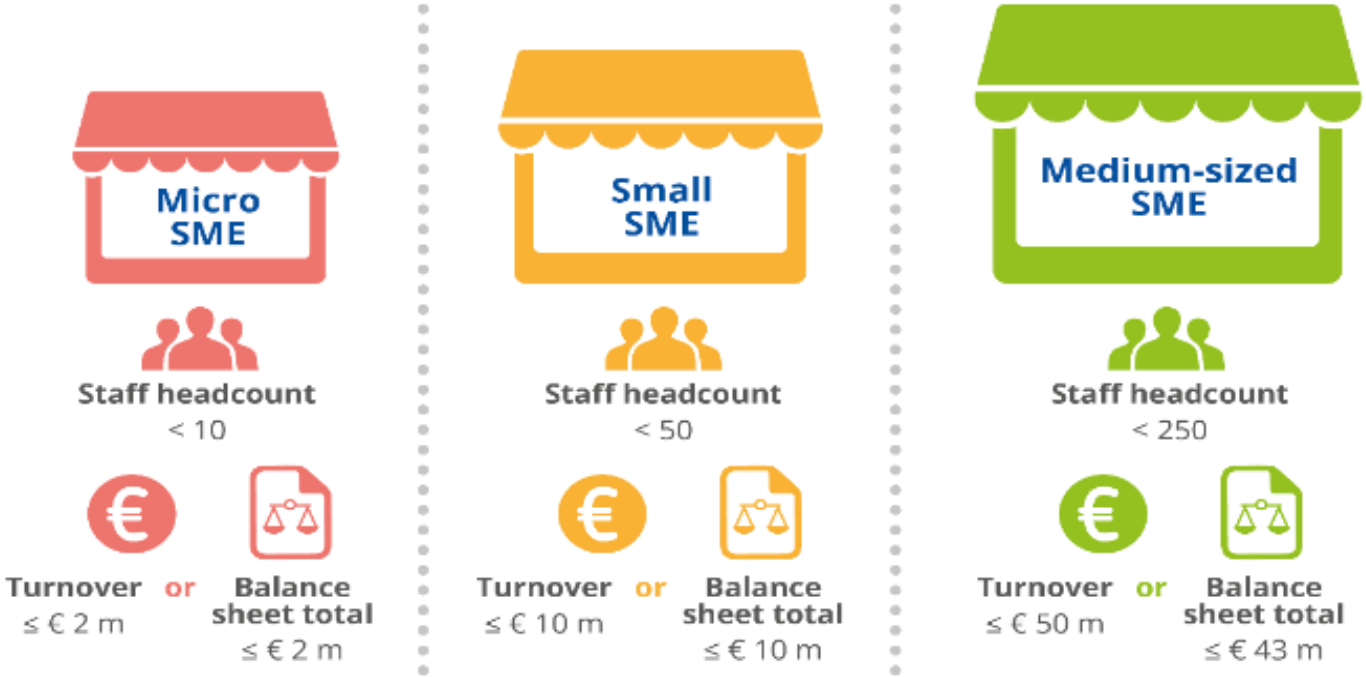
SMES LANDSCAPE

99%

Of businesses in the EU are SMEs

93%

Of SMEs in the EU are micro.



CYBERSECURITY CONCERNS

85%

Cybersecurity a key concern for businesses

84%

OF CYBERATTACKS

rely on social engineering

41% Phising

40% Web based attack

39% General malware

19% Malicious insider

12% Denial of service

11% Social engineering

7% Compromised/ stolen device

TECHNOLOGY USAGE

Figure 8: Use of Cloud

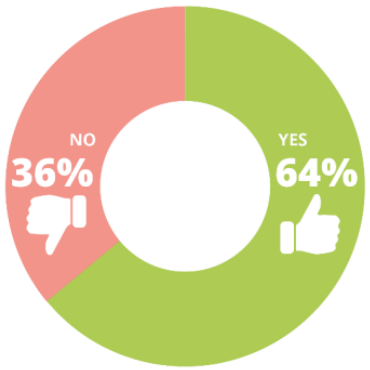
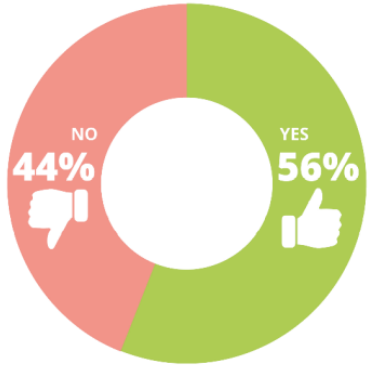


Figure 9: Use of Remote Access



LESS THAN

30%

OF THE PARTICIPANTS

- Removable media management
- ISMS
- Security Officer
- Incident response structure
- Business continuity and Disaster recovery plan
- Cyber/ Information

MORE THAN

70%

OF THE PARTICIPANTS

- Backup
- Antivirus
- Firewall
- Systematic updating of software

CHALLENGES

- Low cybersecurity awareness of the personnel,
- Inadequate protection of critical and sensitive information,
- Lack of budget,
- Lack of ICT cybersecurity specialists,
- Lack of suitable cybersecurity guidelines specific to SMEs,
- Shadow IT, i.e. shift of ICT environment out of SME's control,
- Low management support.
- Compliance with CS legislation

NIS DIRECTIVE IN A NUTSHELL – 3 PILLARS

National capabilities

National capabilities

- National CSIRT
- National authorities
- National cybersecurity strategy
- National cyber crisis management framework

EU collaboration

EU Collaboration

- NIS Cooperation group – strategic collaboration
- EU CSIRTs network - technical collaboration
- EU Cyclone – cyber crisis management coordination
- Coordinated supply chain risk assessments

Supervision of critical sectors

Supervision of critical sectors

- Security measures - risk-based
- Incident reporting - large incidents

NIS2 DIRECTIVE – SECTORS

New but old

IMPORTANT ENTITIES

Annex I "Other Critical Sectors"

or

Annex I "High Criticality" Sector

+

50<employees<250 and
€M10<turnover<€M50

ESSENTIAL ENTITIES

Annex I "High Criticality Sectors"

+

>250 employees and turnover >€M50

or

>€M43 total assets

Essential entities under NIS2	
Digital infrastructures	Telecom networks (mobile, fixed, satellite communications)
	Core internet infrastructure – IXPs, CDNs, TLDs, DNS,
	Trust services (webcertificates, e-signatures)
	Cloud and datacenters
Energy	Electricity
	District heating and cooling
	Oil
	Gas
	Hydrogen
Transport	Air – aviation
	Rail
	Water - Maritime transport, port management, vessel traffic services
	Road – road authorities and intelligent transport systems
Finance	Financial market infra, banking, trading, central counterparties
Health	Health care providers, EU reference laboratories, medicinal research, manufacturing of pharmaceuticals, critical medical devices
Drinking water	Suppliers and distributors
Waste water	Collection, disposal and treatment
Public administration	Central government and regions
Space	Ground-based infrastructure, supporting space-based services
Important entities under NIS2	
Digital providers	Online marketplaces, online search engines, social networks
Postal and courier services	
Waste management	
Chemicals	Manufacturing, production, distribution
Manufacturing	Medical devices, computer, electronic, optical products, electrical equipment, machinery, motor vehicles, other transport equipment

Cloud now critical (ex-ante regime)

New

New

New

New

New

New

New

NIS2 DIRECTIVE – SUPERVISION

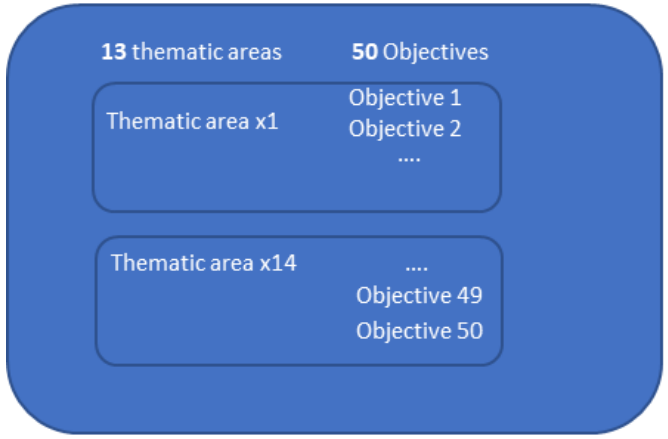
Summary of **Key Similarities and Differences**

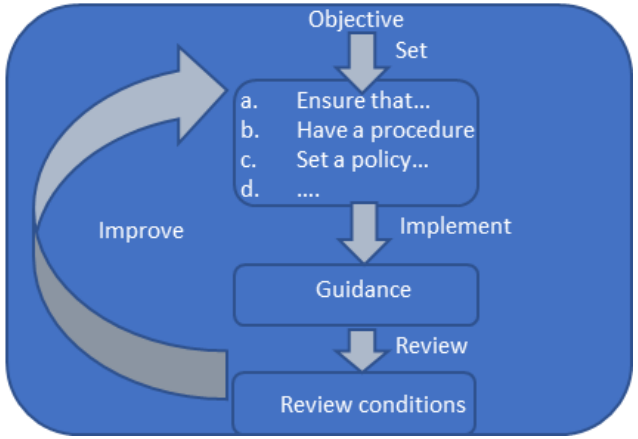
Essential Entities	Important Entities
Obligated to report significant cybersecurity incidents to national authorities.	Obligated to report significant cybersecurity incidents to national authorities.
Regular audits and compliance checks ex ante and ex post	Compliance checks and audits are conducted ex post only
Required to implement robust risk management measures and ensure high levels of cybersecurity resilience.	Required to implement appropriate risk management measures and ensure cybersecurity resilience.

NIS2 SECURITY MEASURES

- ## ENISA has developed a security framework
- Developed with the Member States in the NIS Cooperation Group
- Consulting with several sectorial groups (for instance telecoms)
- Used by the Commission for the implementing acts

- ## Mapping to industry standards
- NIST CSF Framework, ISO 27001/2, ETSI EN 319 401, IEC 62443 family





Governance areas

1. Top management commitment & accountability
2. Network & information security policy
3. Risk management policy
4. Asset management
5. Human resources security
6. Basic cyber hygiene practices & Security training
7. Supply chain security
8. Access control
9. Security in network and information systems acquisition, development & maintenance
10. Cryptography
11. Incident handling
12. Business continuity & crisis management
13. Environmental and physical security

INCIDENT REPORTING (ART. 23)

2 elements that are both to be considered when it comes to defining incidents:

- Event compromising:
  - Availability
  - Authenticity
  - Integrity
  - Confidentiality

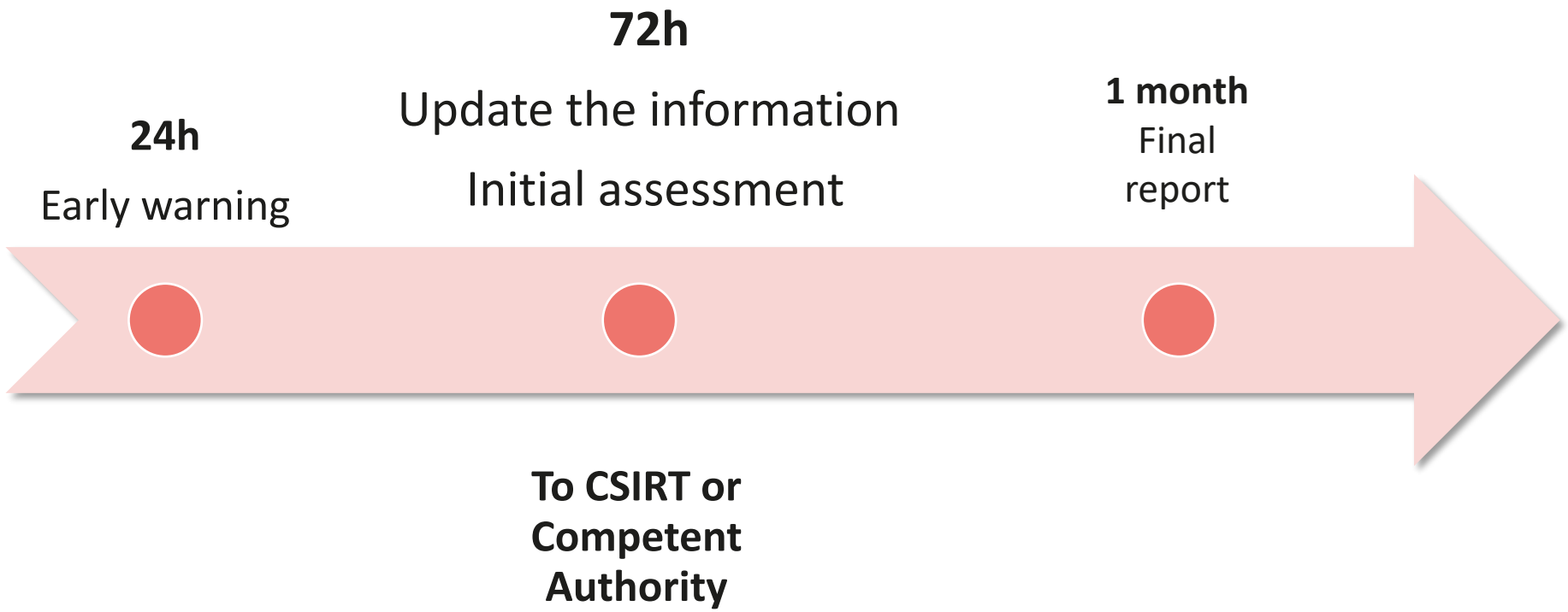
- Event having impact on:
  - Stored, transmitted or processed data
  - Services offered by, or accessible via, network and information systems
  - An event is defined as an incident when it covers any combination of the elements above.

An incident shall be considered to be significant if:
(a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;
(b)it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage

INCIDENT REPORTING

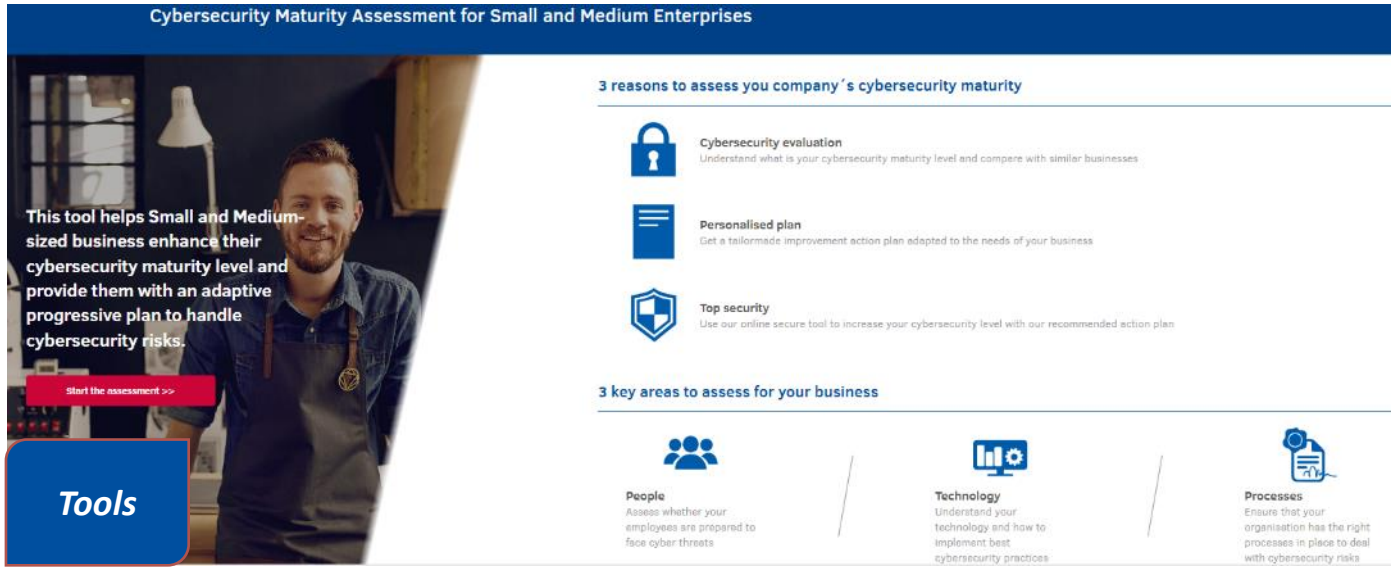
Notification of significant incidents

.



SUPPORTING THE SMEs

Reports



Tools

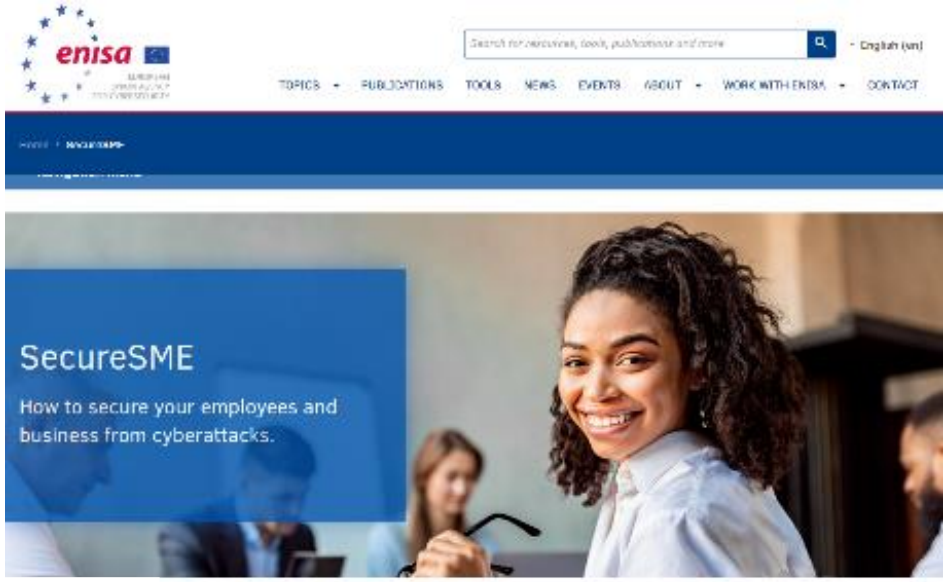
Leaflets

Webinars

PUZZLE

ENISA ACTIONS

Dedicated web tool



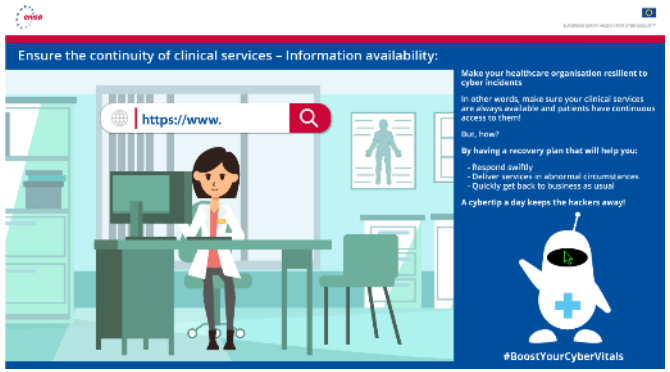
Cybersecurity doesn't necessarily have to be costly for SMEs to implement and maintain. There are several measures that can be implemented, without the company having to invest a large amount.

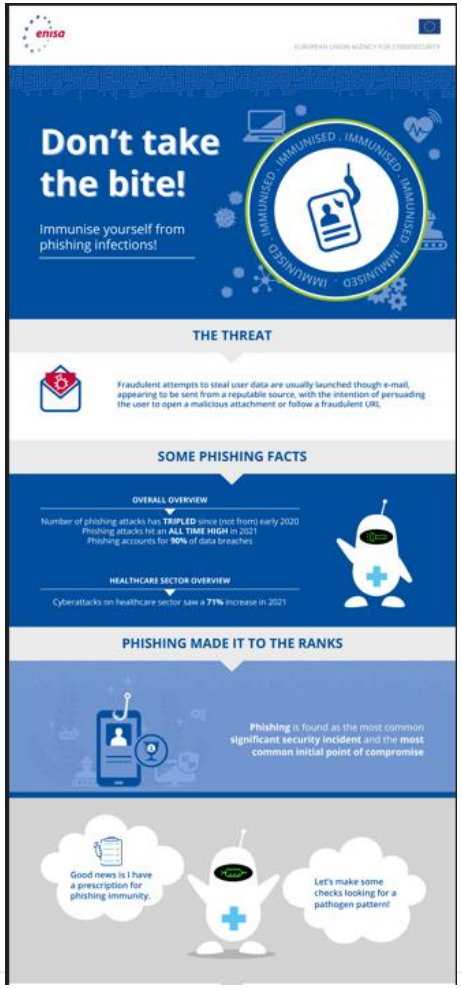
Videos *https://tinyurl.com/2j7rmaj4*

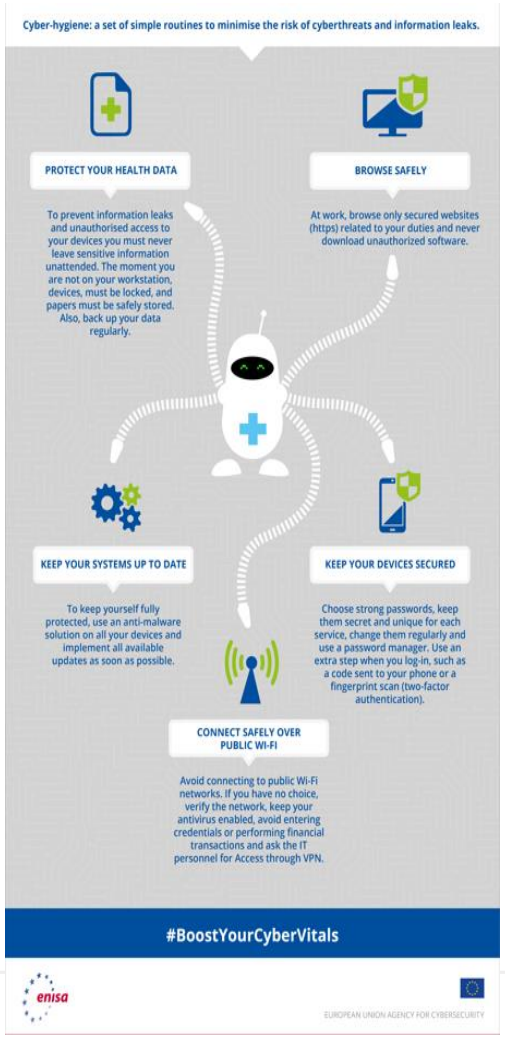
Link to the podcast:
https://www.youtube.com/watch?v=eSuBRO_rawU

Campaigns

HEALTHCARE SECTOR CAMPAIGN

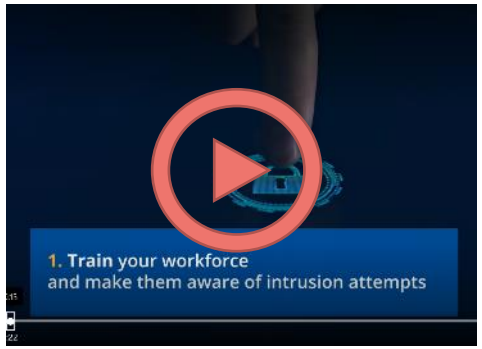


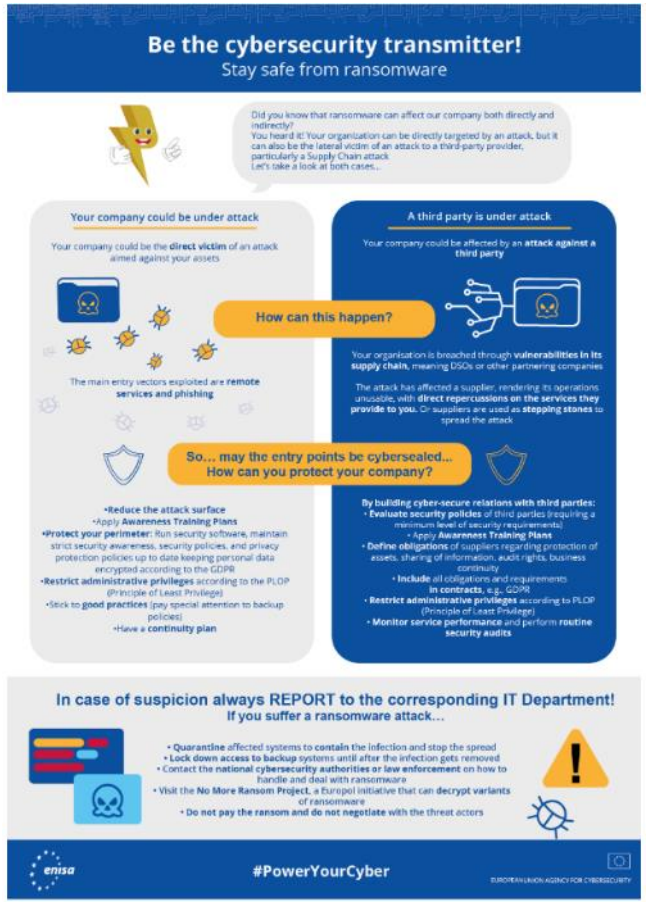




[Cyber Health Week — ENISA (europa.eu)]

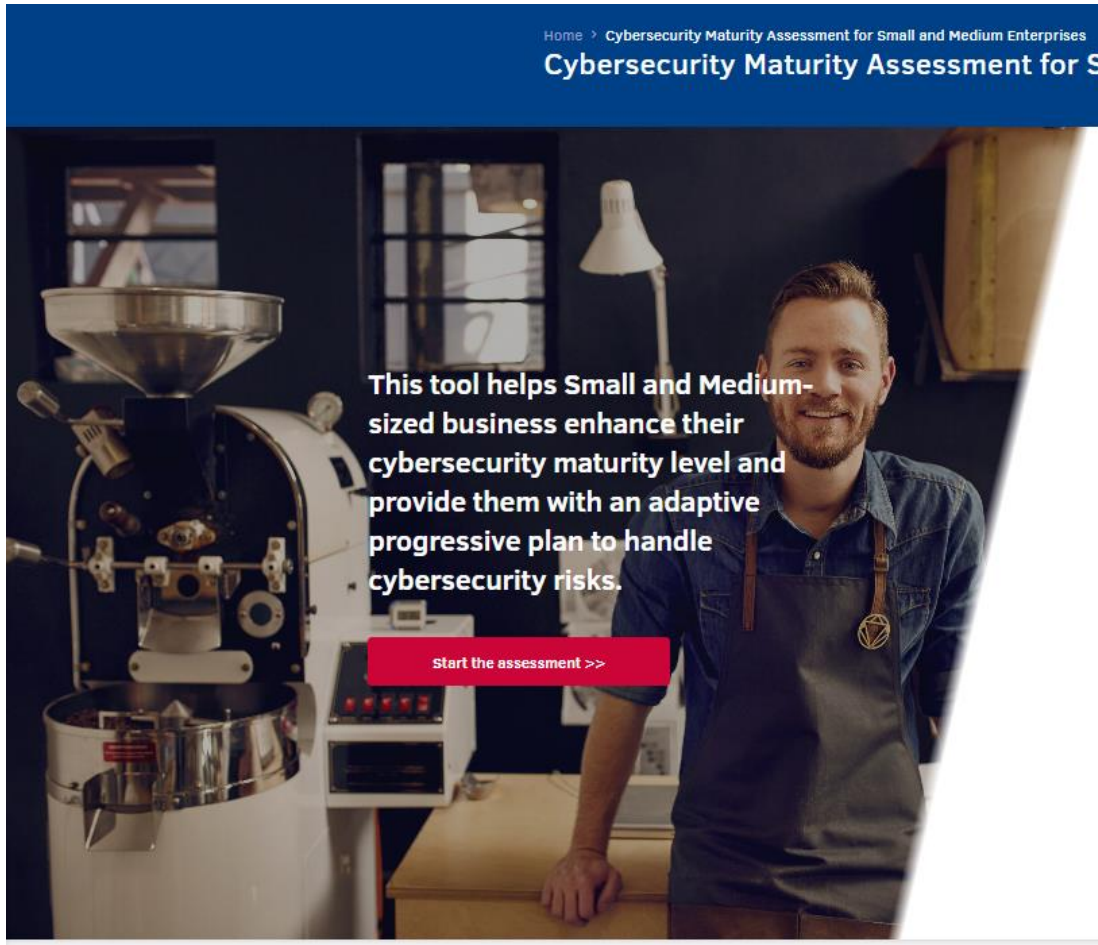
ENERGY CAMPAIGN TO TRANSMISSION SYSTEM OPERATORS



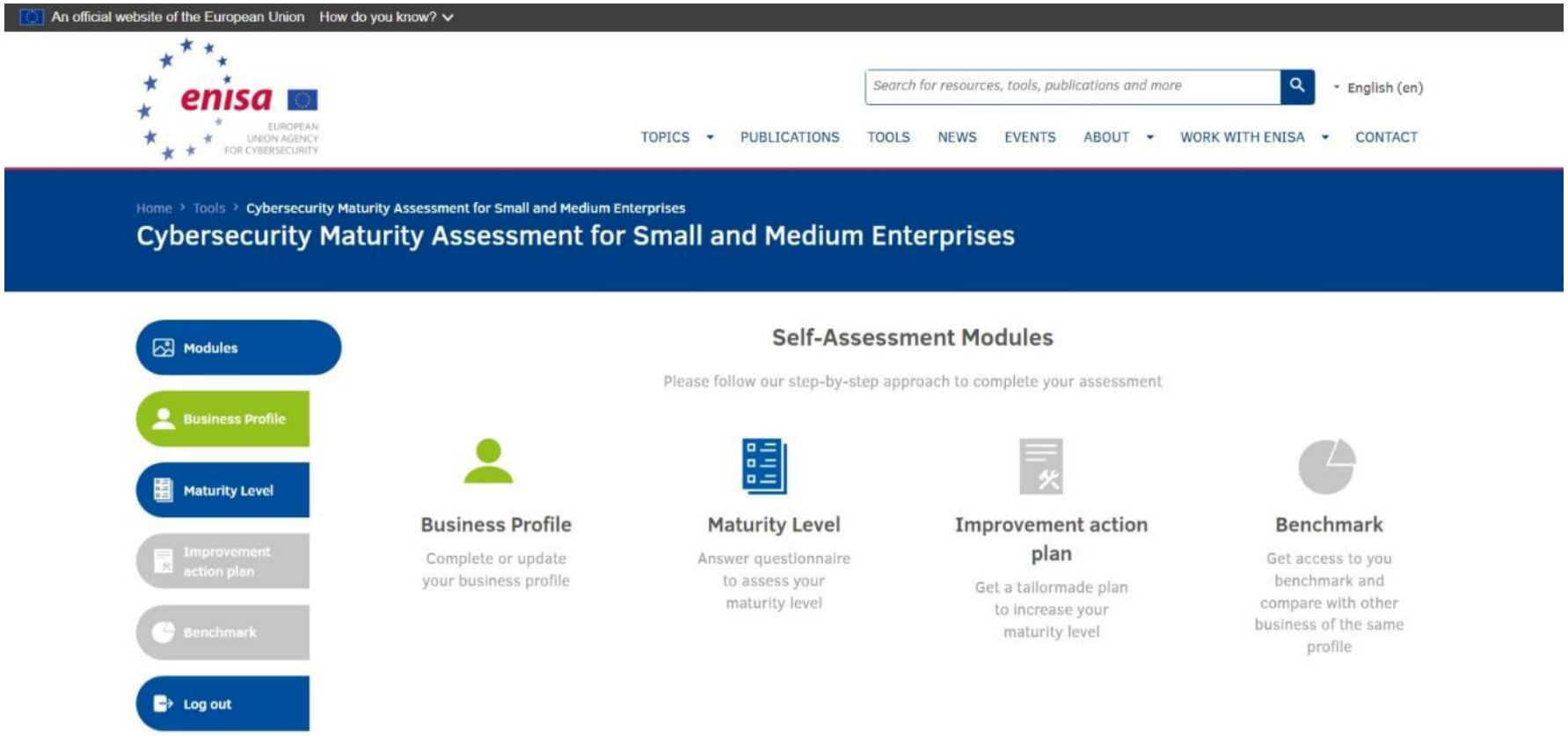


[Cyber Energy Week — ENISA (europa.eu)]

CYBERSECURITY MATURITY ASSESSMENT (CMA)

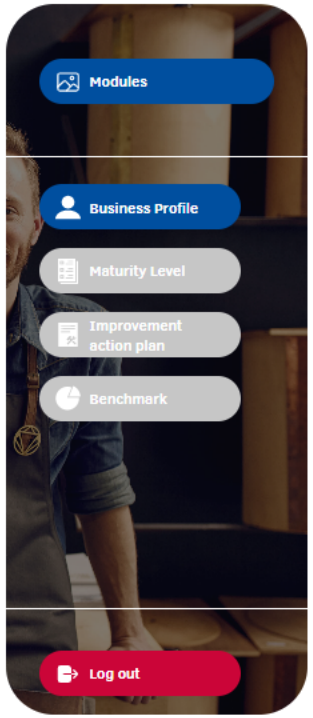


CMA - MODULES



SME Assessment

CMA – ACTION PLAN



Business Profile

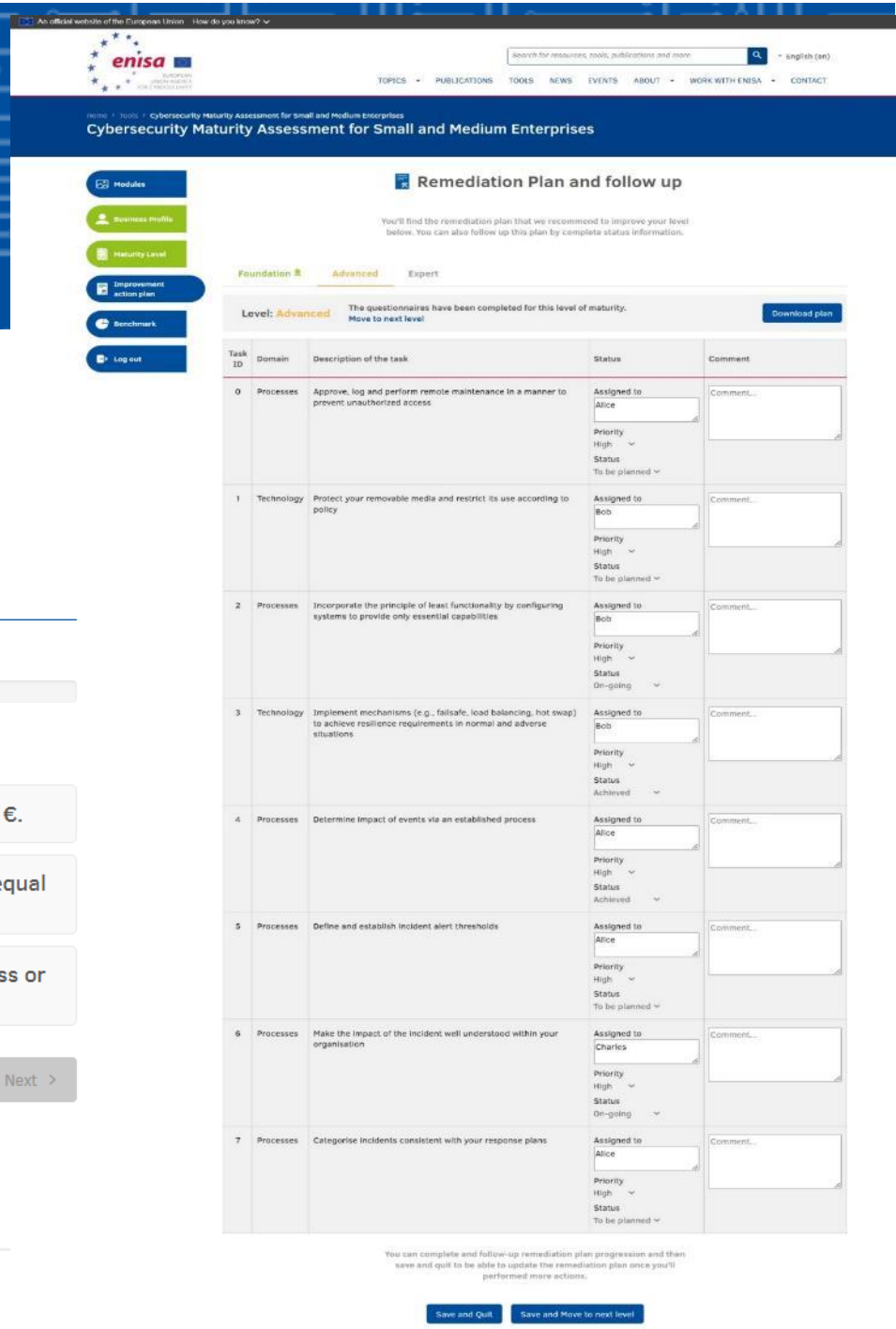
With this profiling questionnaire, information is collected to be able to provide adapted recommendations

Page 1/7 (14%)

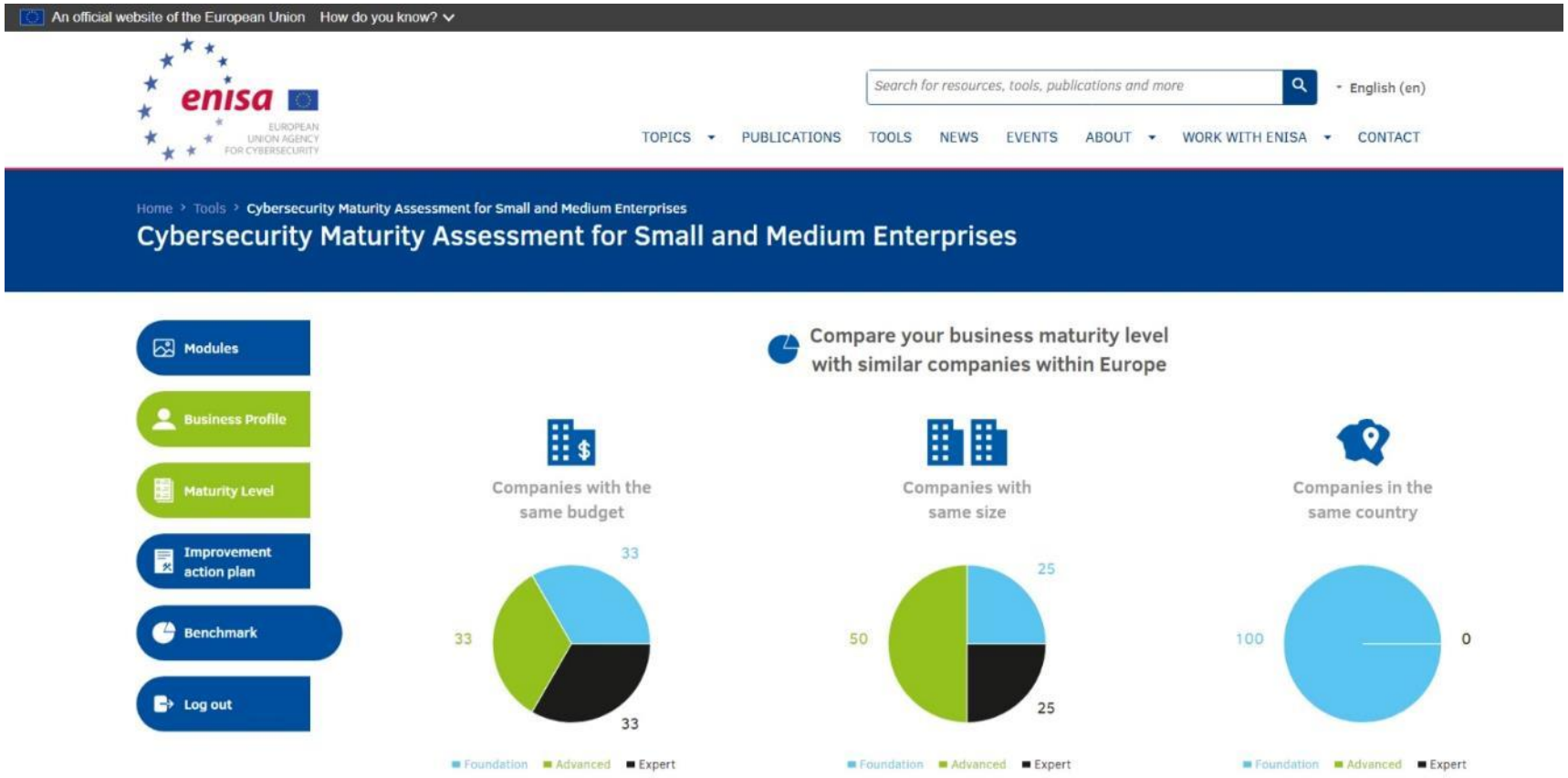
1. **In which size category would you place your company?**

- Micro SMEs : businesses with headcount less than 10 people and annual revenue less or equal to 2m €.
- Small SMEs : businesses with headcount headcount less than 50 people and annual revenue less or equal to 10m €.
- Medium-sized SMEs : businesses with headcount less than 250 staff members and annual revenue less or equal to 50m €.

Previous | Save and quit | Next



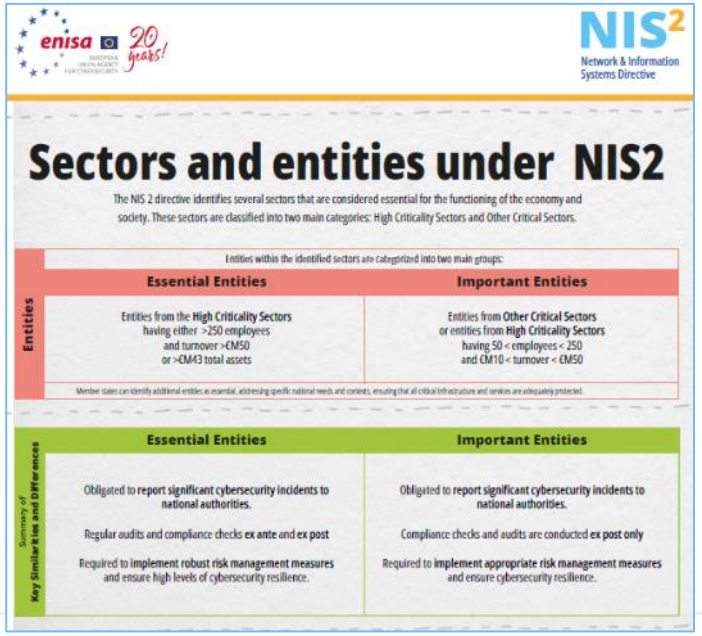
CMA - BENCHMARK



THE WAY FORWARD

NEXT STEPS

- Measure the maturity of SMEs and analyze further challenges they face
- NIS2 awareness campaigns



THE WAY FORWARD

NEXT STEPS

- AR-in-a-Box for SMEs!

for SMEs

THANK YOU FOR YOUR ATTENTION

Agamemnonos 14, Chalandri 15231
Attiki, Greece

info@enisa.europa.eu

www.enisa.europa.eu