GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE ECONOMÍA Y APOYO A LA EMPRESA
DIRECCIÓN GENERAL DE SEGUROS Y FONDOS DE PENSIONES

Cybersecurity: new challenges for supervisors and insurance market

Mónica González Perdiguero

Dirección General de Seguros
y Fondos de Pensiones

ASSAL, 2 May 2023

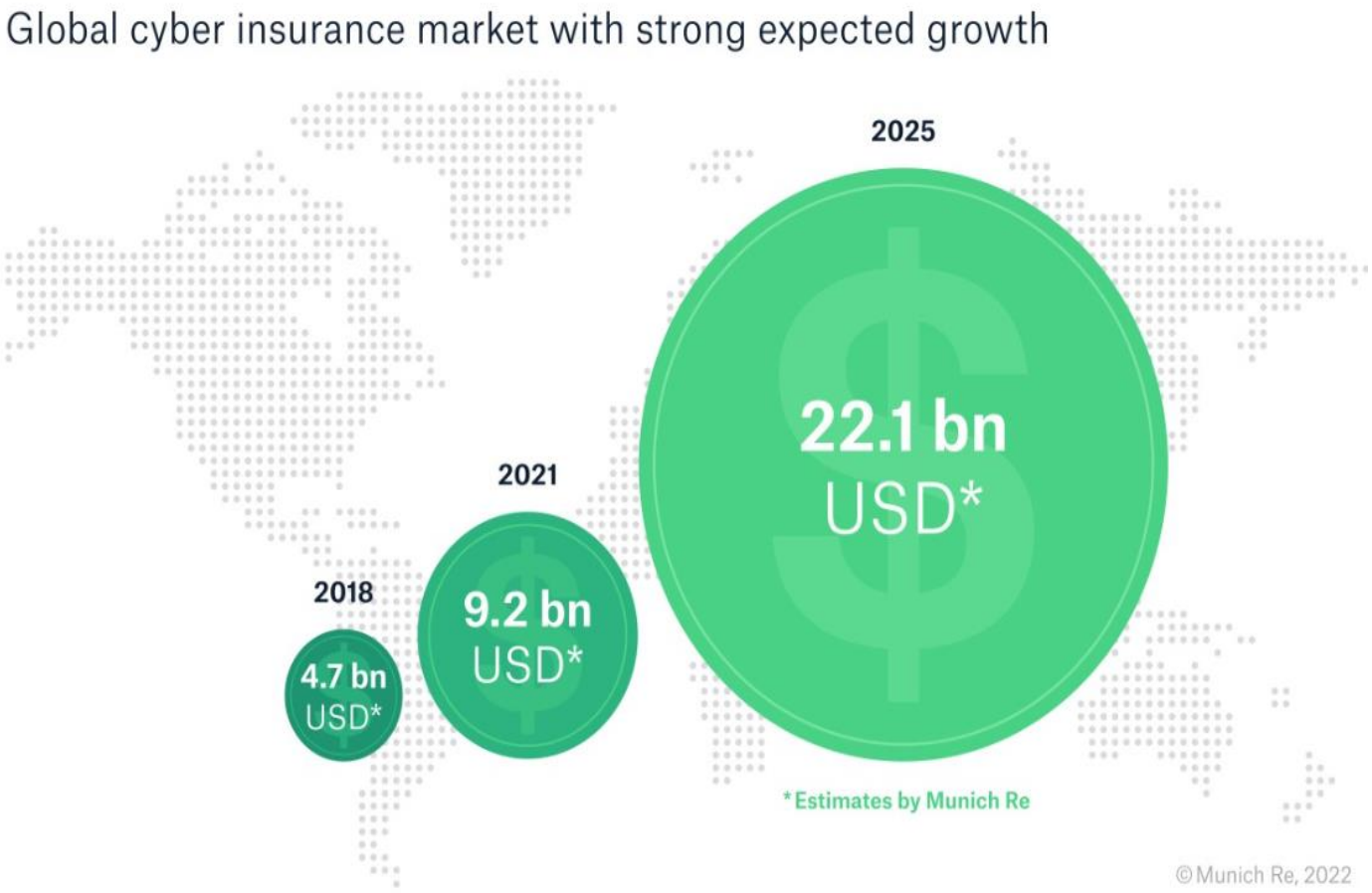
1. Cyber risk as underwriting risk

2. Challenges for supervision

1. Cyber risk as underwriting risk

- Background: accelerators
  - Digitalisation and interconnectivity
  - Covid outbreak
  - Russia invasion of Ukraine

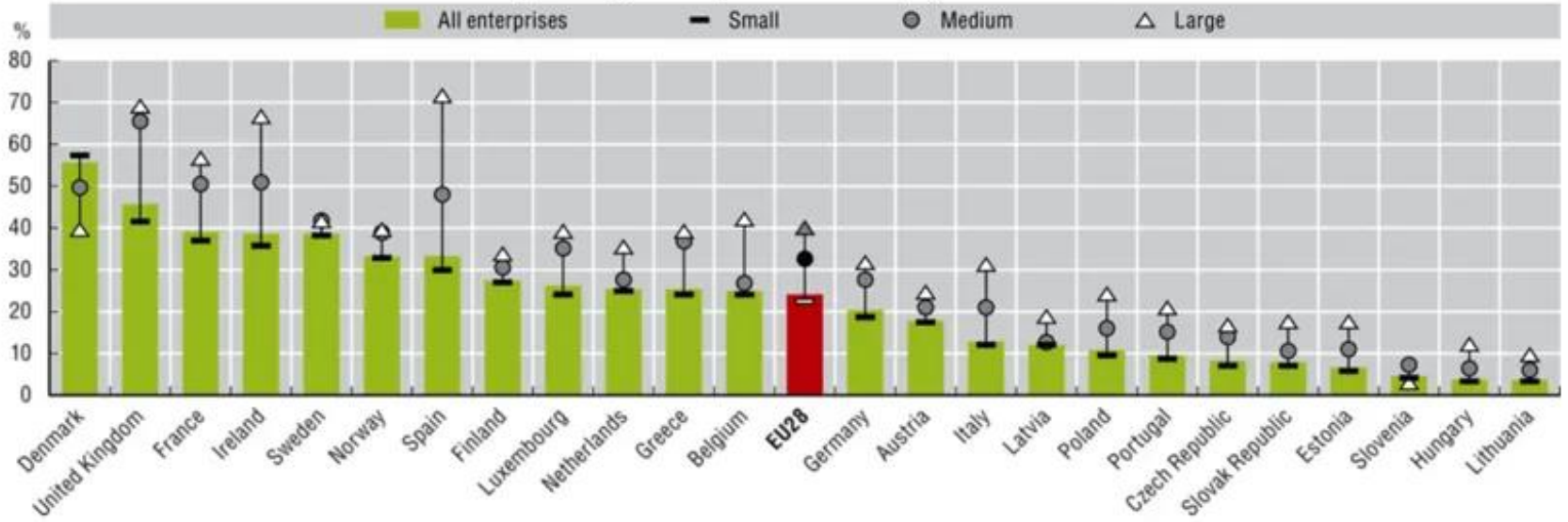
Cyber insurance market



Spain is the European country with the most large enterprises covered against cyber incidents

Figure 7.4. **Enterprises with insurance against ICT security incidents by size, 2019**

As a percentage of enterprises in each employment size class



- Cyber risks:
  - Affirmative cyber risks: instances where cyber risks are included within an insurance policy
  - Non-affirmative cyber risks: instances where cyber exposure is neither explicitly included nor excluded within an insurance policy

2. Challenges for supervision

- Cyber attacks suffered by insurers
- Supervision of cyber risks management

Insurers face cyber attacks…

El Confidencial

España Cotizalia Opinión Salud Internacional Cultura Teknautas Deportes ACyV Televisión Vani

A LA VENTA EN LA 'DARK WEB'

Agujero de seguridad en Zurich Seguros: roban y difunden los datos de sus clientes en España

Un grupo de ciberdelincuentes ha robado los datos de los clientes de Zurich Seguros en España. La noticia, adelantada por este periódico, ha sido confirmada por la compañía

AR SESIÓN

CRÓNICA CREACIÓN

Sede de Generali en Madrid / EP

Generali reconoce un ciberataque contra sus sistemas informáticos

La aseguradora alerta a sus exclientes de un "acceso ilegítimo" registrado el pasado fin de semana y que ya ha sido resuelto

BUSINESS INSURANCE

RISK MANAGEMENT WORKERS COMP INTERNATIONAL RESEARCH & REPOR

International

Mapfre hit by cyber attack

August 17, 2020

SHARE

Spain-based insurer Mapfre SA suffered a cyber attack in the weekend of Aug. 15, El Pais reported. No data was stolen in the attack, which slowed down the systems, the company said.

Reputational damage

- The reputational damage may also be substantial or even irreversible.

- Some insurers, in Spain and in other countries, cover the reputational costs caused by the cyber incident.

- Regulation in Europe and Spain

	EIOPA	DORA	TIBER-ES
Requisitos relacionados con la gobernanza	Directriz 1, 2	Art 4	-
Requisitos de gestión del riesgo de TIC	Directriz 1, 2, 4 a 6, 12 a 14, 16, 18, 21 y 22	Art 5 a 14	-
Notificación de incidentes relacionados con las TIC	Directriz 4, 7 , 11, 12, 15, 17, 22, 24, 25	Art 15 a 20	-
Pruebas de resiliencia operativa digital	Directriz 12, 14, 17, 22, 23	Art 21 a 24	Pruebas avanzadas de penetración (Red Team)
Riesgo de terceros relacionado con las TIC	-	Art 25 a 39	-
Intercambio de información	-	Art 40	-

- EIOPA Guidelines adopted in October 2020

EIOPA-BoS-20/600

Guidelines on information and communication technology security and governance

https://www.eiopa.europa.eu/system/files/2020-10/eiopa-bos-20-600-guidelines-ict-security-and-governance.pdf

Guidelines on information and communication technology security and governance

The objective of these Guidelines is to:

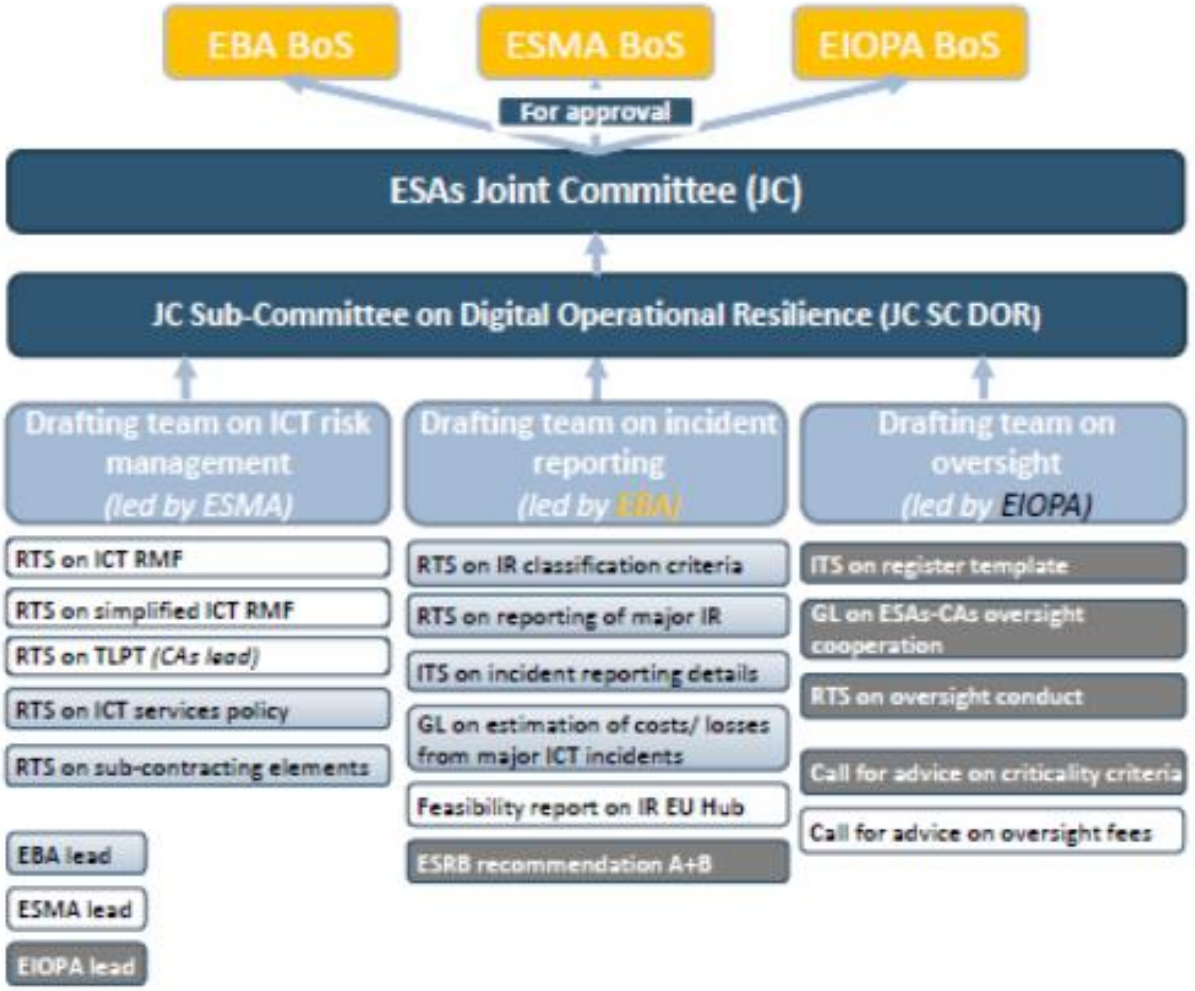
a) provide clarification and transparency to market participants on the minimum expected information and cyber security capabilities, i.e. security baseline;

b) avoid potential regulatory arbitrage;

c) foster supervisory convergence regarding the expectations and processes applicable in relation to ICT security and governance as a key to proper ICT and security risk management.

- REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on digital operational resilience for the financial sector

- New rules in preparation



EUROPEAN CENTRAL BANK

EUROSYSTEM

TIBER-EU FRAMEWORK

How to implement the European framework for Threat Intelligence-based Ethical Red Teaming

- TIBER-EU is a common framework that delivers a controlled, bespoke, intelligence-led red team test of entities' critical live production systems. Intelligence-led **red team** tests mimic the tactics, techniques and procedures (TTPs) of real-life threat actors who, on the basis of threat intelligence, are perceived as posing a genuine threat to entities.

- An intelligence-led red team test involves the use of a variety of techniques to simulate an attack on an **entity's critical functions** (CFs) and underlying systems (i.e. its people, processes and technologies).

- It helps an entity to assess its protection, detection and response capabilities.

From TIBER – EU to TIBER – ES

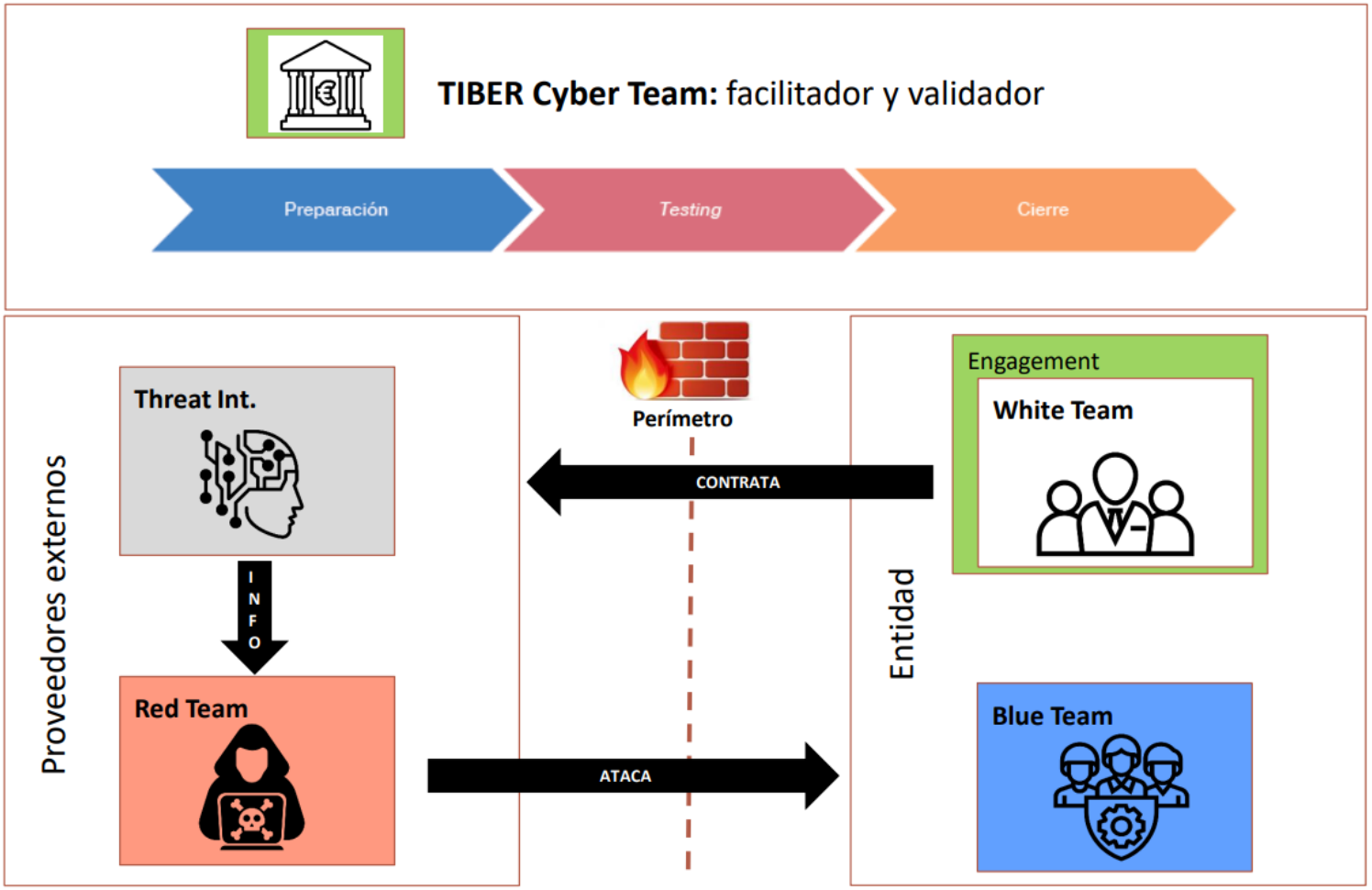
In **2018**, **TIBER-EU** became the first EU framework for cibersecurity tests

↓

The Bank of Spain adopted its local framework in **december 2020: TIBER – ES**

↓

The **implementation guide** for TIBER – ES was published in **december 2021**

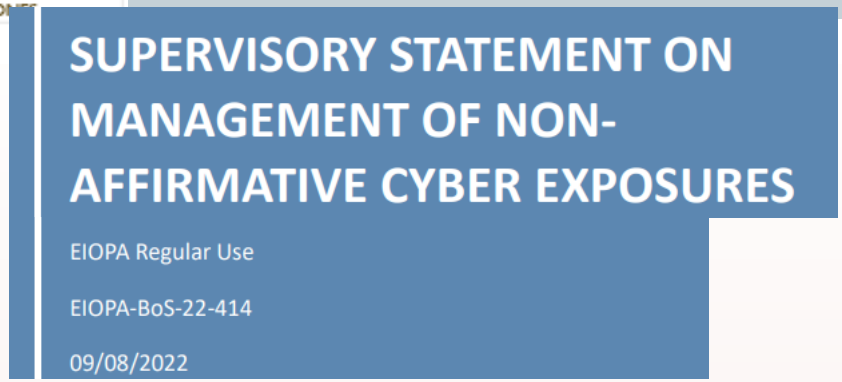

TIBER Cyber Team: facilitador y validador
Preparación
Testing
Cierre
Proveedores externos
Threat Int.
INFO
Red Team
Perímetro
CONTRATA
ATACA
Entidad
Engagement
White Team
Blue Team

EIOPA's second Report Cyber Risks for Insurers – Challenges and Opportunities (2019)

''Although still small in size, the European cyber insurance industry is growing rapidly. At the same time, non-affirmative cyber exposures remain a source of concern. While common efforts to assess and address non-affirmative cyber risks are under way, the lack of quantitative approaches, explicit cyber exclusions and action plans to address non-affirmative cyber exposures suggest insurers are currently not fully aware of the potential exposures to cyber risk.''

Silent cyber risks:

https://www.eiopa.europa.eu/system/files/2022-09/supervisory_statement_on_management_of_non-affirmative_cyber_exposures.pdf



EIOPA published a Supervisory Statement on non-affirmative cyber risk and cyber insurance exclusions to provide clarity on the management and underwriting of nonaffirmative cyber insurance risk.

EIOPA believed that without the introduction of this additional policy, the previous status quo would have failed to provide an adequate regulatory and supervisory framework for (re)insurance undertaking and the supervisory authorities in their handling of non-affirmative cyber insurance risk. Moreover, the entire industry would have faced the risk to develop non-homogenous practices and apply them in a non-homogeneous pattern harming the goal of achieving a level playing field with respect to sound cyber underwriting and cyber risk management practices.

Finally, given the potentially systemic nature of cyber threats, not issuing proper policy action on the topic could increase the impact of operational risks overall for the entire industry, with potential impacts on undertakings and policyholders.

Thank you very much for your attention